FortiGate™

Version 4.0 MR1

CLI Reference

FORTINET
UNIFIED THREAT MANAGEMENT SOLUTIONS

FortiGate CLI Reference

Version 4.0 MR1

19 October 2009

01-401-93051-20091019

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Contents

Introduction

This chapter introduces you to the FortiGate Unified Threat Management System and the following topics:

About the FortiGate Unified Threat Management System

The FortiGate Unified Threat Management System supports network-based deployment of application-level services, including virus protection and full-scan content filtering. FortiGate units improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network.

The FortiGate unit is a dedicated easily managed security device that delivers a full suite of capabilities that include:

- application-level services such as virus protection and content filtering,
- network-level services such as firewall, intrusion detection, VPN, and traffic shaping.

The FortiGate unit employs Fortinet's Accelerated Behavior and Content Analysis System (ABACAS™) technology, which leverages breakthroughs in chip design, networking, security, and content analysis. The unique ASIC-based architecture analyzes content and behavior in real-time, enabling key applications to be deployed right at the network edge where they are most effective at protecting your networks. The FortiGate series complements existing solutions, such as host-based antivirus protection, and enables new applications and services while greatly lowering costs for equipment, administration, and maintenance.

Registering your Fortinet product

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Center article Registration Frequently Asked Questions.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Center article What does Fortinet Technical Support require in order to best assist the customer?

Fortinet documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

Fortinet Knowledge Center

The Fortinet Knowledge Center provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Center at http://kc.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

CLI constraints

CLI constraints, such as <address_ipv4>, indicate which data types or string patterns are acceptable input for a given parameter or variable value. CLI constraint conventions are described in the CLI Reference document for each product.

Notes, Tips and Cautions

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.

Tip: Highlights useful additional information, often tailored to your workplace activity.

Note: Also presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From *Minimum log level*, select *Notification*.

CLI input	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FGT-602803030703 # get system settings`
	`comments  : (null)`
	`opmode  : nat`

Emphasis	HTTP connections are ***not*** secure and can be intercepted by a third party.
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>` `<BODY><H4>You must authenticate to use this service.</H4>`
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com.
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Navigation	Go to *VPN* > *IPSEC* > *Auto Key (IKE)*.
Publication	For details, see the *FortiGate Administration Guide*.

What's new

The table below lists commands that have changed since the previous release, version 4.0.

Note: There are some changes in terminology in this *CLI Reference* intended to make syntax descriptions more accurate and consistent. Mainly, the term "keyword" has been replaced by the terms "field", "option", and "value". A field can be set to either an entered value, such as an IP address, or to one of several fixed named options. For detailed information, see "Command syntax" on page 35.

Command	Change
`config application list`	
`edit <app_list_str>`	
`config entries`	
`edit <id_integer>`	
`set open-contact-pinhole`	New field to open or close SIP pinholes for non-REGISTER SIP requests (usually INVITE requests).
`set open-register-pinhole`	New field to open or close SIP pinholes for SIP REGISTER requests.
`set rfc2543-branch`	New field to support RFC 2543-complaint SIP calls involving branch commands that are missing or that are valid for RFC 2543 but are invalid for RFC 3261.

`set sccp-archive-full`
`set sccp-archive-summary`
`set simple-archive-full`
`set simple-archive-summary`
`set sip-archive-summary`
`set sip-archive-full`
	fields removed.

`config dlp rule`	
`edit rule_name`	
`set field`	New option `always`. Matches all transfers.
`set protocol`	New option `session-ctrl`.
`config dlp sensor`	
`config rule`	
`edit <rule_str>`	
`set archive`	New option `summary-only` enables summary DLP archiving for the rule or compound rule.
`set severity`	New field. An integer from 1 to 5 to indicate the seriousness of the problems that would result from the content passing through the FortiGate unit.
`config endpoint-control apps-detection`	Renamed to `config endpoint-control apps-detect rule-list`
`config endpoint-control apps-detect rule-list rule-list`	Renamed from `config endpoint-control apps-detection`
`config endpoint-control profile`	New command. Configures an Endpoint NAC profile.

Command	Change
config endpoint-control settings	
set compliance-timeout	New field. Sets the authentication timeout for compliant endpoints.
set enforce-minimum-version	New field. Requires endpoints to run a defined minimum version of FortiClient Host Security.
config firewall address, address6	
edit <name_str>	
set cache-ttl	New field. Sets minimum time-to-live (TTL) of individual IP addresses in FQDN cache.
config firewall interface-policy	
edit <policy_id>	
set application-list	New field. Specifies the application black/white list the FortiGate unit uses when examining network traffic.
set application-list-status	New field. Enables use of application black/white list on matching network traffic.
config firewall interface-policy6	
edit <policy_id>	
set application-list	New field. Specifies the application black/white list the FortiGate unit uses when examining network traffic.
set application-list-status	New field. Enables use of application black/white list on matching network traffic.
config firewall ippool	
edit <index_int>	
set interface	Field removed.
config firewall policy, policy6	
edit <index_int>	
set endpoint-allow-collect-sysinfo set endpoint-redir-portal set endpoint-restrict-check	Fields removed.
set endpoint-profile	New field. Specifies which endpoint NAC profile to apply.
config firewall profile	
edit <profile_str>	
set ftp archive-full set ftp archive-summary	Options removed. Archiving is now part of Data Leak Prevention.
set ftp scanextended	Option removed. Use ftp-avdb field to select normal or extended database for AV scan.
set ftp-avdb	New field. Select normal or extended AV database for FTP traffic. Replaces scanextended option.
set http content-type check	New option.
set http scanextended	Option removed. Use http-avdb field to select normal or extended database for AV scan.
set http-avdb	New field. Select normal or extended AV database for HTTP traffic. Replaces scanextended option.
set http-post-lang	New field. Specifies up to five character set encodings to use when applying spam filtering banned word checking, web filtering or DLP content scanning.
set https-avdb	New field. Select normal or extended AV database for HTTPS traffic. Replaces scanextended option.

Command	Change
config firewall profile (continued)	
edit <profile_str>	
set im scanextended	Option removed. Use im-avdb field to select normal or extended database for AV scan.
set im-avdb	New field. Select normal or extended AV database for IM traffic. Replaces scanextended option.
set imap archive-full set imap archive-summary	Options removed. Archiving is now part of Data Leak Prevention.
set imap scanextended	Option removed. Use imap-avdb field to select normal or extended database for AV scan.
set imap-avdb	New field. Select normal or extended AV database for IMAP traffic. Replaces scanextended option.
set imaps archive-full set imaps archive-summary	Options removed. Archiving is now part of Data Leak Prevention.
set imaps scanextended	Option removed. Use imaps-avdb field to select normal or extended database for AV scan.
set imaps-avdb	New field. Select normal or extended AV database for IMAPS traffic. Replaces scanextended option.
set nntp archive-full set nntp archive-summary	Options removed. Archiving is now part of Data Leak Prevention.
set nntp quarantine	New option. Quarantines infected files.
set nntp scanextended	Option removed. Use nntp-avdb field to select normal or extended database for AV scan.
set nntp-avdb	New field. Select normal or extended AV database for NNTP traffic. Replaces scanextended option.
set per-ip-shaper	New field. Specifies the per-IP traffic shaper to apply.
set pop3 scanextended	Option removed. Use pop3-avdb field to select normal or extended database for AV scan.
set pop3-avdb	New field. Select normal or extended AV database for POP3 traffic. Replaces scanextended option.
set pop3s scanextended	Option removed. Use pop3s-avdb field to select normal or extended database for AV scan.
set pop3s-avdb	New field. Select normal or extended AV database for POP3S traffic. Replaces scanextended option.
set safesearch	New field. Enforces use of safe search feature on Google, Yahoo, or Bing search engines.
set smtp scanextended	Option removed. Use smtp-avdb field to select normal or extended database for AV scan.
set smtp-avdb	New field. Select normal or extended AV database for SMTP traffic. Replaces scanextended option.
set smtps scanextended	Option removed. Use smtps-avdb field to select normal or extended database for AV scan.
set smtps-avdb	New field. Select normal or extended AV database for SMTPS traffic. Replaces scanextended option.
config log set log-im set log-p2p set log-voip set log-violations	Fields removed.
config firewall schedule group	New command. Configures schedule groups.

Command	Change
`config firewall shaper per-ip-shaper`	New command. Configures traffic shaping that is applied per IP address, instead of per policy or per shaper.
`config firewall shaper traffic-shaper`	Renamed from `config firewall traffic-shaper`.
`edit <name_str>`	
`set action`	New field. Selects traffic accounting logging or blocking or traffic exceeding the quota.
`set quota`	New field. Sets the traffic quota.
`set type`	New field. Selects hourly, daily, weekly or monthly period for accounting logs or traffic quota enforcement.
`config firewall sniff-interface-policy` `config firewall sniff-interface-policy6`	New commands. Configure FortiGate unit interface to operate as a one-arm intrusion detection system (IDS) appliance.
`config firewall traffic-shaper`	Renamed `config firewall shaper traffic-shaper`.
`config log disk setting`	
`set sql-max-size`	New field. Sets maximum size of SQL logs.
`set sql-max-size-action`	New field. Selects action when maximum log size is reached.
`set sql-oldest-entry`	New field. Sets number of days to keep log entries.
`config sql-logging`	New subcommand. Enables or disables SQL logging by log type.
`config log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting`	
`set wanopt-traffic`	New field. Enables WAN optimization traffic logging.
`set webcache-traffic`	New field. Enables WAN optimization web caching traffic logging.
`config log {fortianalyzer | syslogd} override-filter`	New command. Overrides the global configuration created with the `config log {fortianalyzer | syslogd} filter` command.
`config log fortianalyzer override-setting`	New command. Overrides the global configuration created with the `config log fortianalyzer setting` command.
`config log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting`	Renamed from `config system fortianalyzer`.
`set address-mode`	New field. Selects auto-discovery or static addressing.
`set conn-timeout`	New field. Sets the FortiAnalyzer connection timeout.
`set encrypt`	New field. Enables use of IPSec VPN tunnel for communication.
`set fdp-device`	New field. Sets serial number of the Fortianalyzer unit.
`set localid`	New field. Sets the identifier that both FortiGate and FortiAnalyzer units use.
`set psksecret`	New field. Sets the pre-shared key for the IPSec VPN tunnel.
`set server`	New field. Sets the IP address of the FortiAnalyzer unit.
`set ver-1`	Field removed.
`config log syslogd override-setting`	New command. Overrides for this VDOM the global configuration created with the `config log syslogd setting` command.
`config log {syslogd | syslogd2 | syslogd3} setting`	
`set reliable`	New field. Enables reliable delivery of syslog messages in compliance with RFC 3195.
`config report ...`	New commands. Configure log reports.

Command	Change
config router access-list, access-list6	New command (access-list6).
config router bgp	
config aggregate-address6	New subcommand. IPv6 version of config aggregate-address.
config neighbor	Many IPv6 fields added. All end with "6".
config network6	New subcommand. IPv6 version of config network.
config redistribute6	New subcommand. IPv6 version of config redistribute.
config router prefix-list, prefix-list6	New command (prefix-list6). IPv6 version of prefix-list.
config router ripng	New command. Configures the "next generation" Routing Information Protocol, RIPng.
config router static	
edit <sequence_number>	
set weight	New field. Adds weights to ECMP static routes if the ECMP route failover and load balance method is set to weighted.
config spamfilter ipbwl	
config entries	
set addr-type	New field. Selects IPv4 or IPv6 addressing.
set ip4-subnet	New field. Specifies IPv4 trusted address.
set ip6-subnet	New field. Specifies IPv6 trusted address.
set ip/subnet	Field replaced by ip4-subnet and ip6-subnet.
config spamfilter iptrust	
config entries	
set addr-type	New field. Selects IPv4 or IPv6 addressing.
set ip4-subnet	New field. Specifies IPv4 trusted address.
set ip6-subnet	New field. Specifies IPv6 trusted address.
set ip/subnet	Field replaced by ip4-subnet and ip6-subnet.
config system admin	
edit <name_str>	
set force-password-change	New field. Requires this administrator to change password at next login.
set ip6-trusthost1 set ip6-trusthost2 set ip6-trusthost3	New fields. Set IPv6 trusted hosts.
set moduleid	Field removed.
set password-expire	New field. Sets a date and time for password expiry.
config system dns	
set autosvr	Field removed
set fwdintf	Field removed
config system dns-database	New command. Configures the FortiGate DNS database.
config system fortianalyzer config system fortianalyzer2 config system fortianalyzer3	Commands renamed config log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting.

Command	Change
config system fortiguard	
config serv-ovrd-list	
set addr-type	New field. Selects IPv4 or IPv6 addressing.
set ip6	New field. IPv6 version of ip.
config system global	
set anti-replay	New field. Sets level of protection against packet replay exploits. Replaces conn-tracking.
set conn-tracking	Replaced by anti-replay.
set registration-notification	New field. Enables displaying the registration notification in the web-based manager if the FortiGate unit is not registered.
set internal-switch-mode {hub | interface | switch}	New hub option for enabling hub mode which is similar to switch mode.
set log-user-in-upper	New field. Enables logging of user name in upper case.
set service-expire-notification	New field. Enables displaying a notification on the web-based manager 30 days before the FortiGate unit support contract expires.
set wireless-controller	New field. Enables wireless controller feature.
set wireless-controller-port	New field. Sets control and data ports for wireless controller mode.
set wireless-terminal	New field. Enables FortiWiFi unit to be managed by another FortiGate unit's wireless controller feature.
set wireless-terminal-port	New field. Sets control and data ports for wireless terminal mode.
config system interface	
edit <interface_name>	
set detectprotocol	New field. Selects the protocols to use to detect interface connection status.
set dhcp-client-identifier	New field. Change the default DHCP client identifier.
set dns-query	New field. Configures interface to accept DNS queries, recursive or non-recursive.
set explicit-web-proxy	New field. Enables explicit web proxy on this interface.
set spillover-threshold	New field. Limits the amount of bandwidth processed by the Interface.
config system modem	
set authtype1 set authtype2 set authtype3	New fields. Sets the authentication methods to use for 3G modems.
set wireless-port	New field. Sets TTY Port for 3G modems.
config system password-policy	New command. Configures higher security requirements for administrator passwords and IPsec VPN pre-shared keys.
config system replacemsg ec	Changed command. Now also configures Endpoint NAC Recommendation Portal.
config system replacemsg traffic-quota	New command. Formats traffic shaping quota replacement messages.
config system replacemsg-group	New command. Defines replacement messages for your VDOM, overriding global replacement messages.
config system settings	
set v4-ecmp-mode	New field. Sets the ECMP route failover and load balance method.

Command	Change
config system snmp sysinfo	
set engine-id	New field. Sets optional engine-id string for snmpEngineID.
config system snmp user	
edit <username>	
set auth-proto	New field. Selects authentication protocol.
set auth-pwd	New field. Sets user's password.
set priv-proto	New field. Selects privacy (encryption) protocol.
set priv-pwd	New field. Sets the privacy encryption key.
set security-level	New field. Enables authentication and privacy.
config system wireless settings	
set geography	Default changed from World to Americas.
config user group	
edit <groupname>	
set ldap-memberof	New field. Specifies the LDAP groups to which members of this user group belong.
config user peer	
edit <peer_name>	
set password	New field. Sets password for two-factor authentication.
set two-factor	New field. Enables two-factor authentication.
config user setting	
set auth-blackout-time	New field. Sets blackout time for failed user authentication attempts.
set auth-http-basic	New field. Enables HTTP basic authentication for identify-based firewall policies.
config auth-ports	New subcommand. Configures non-standard ports for firewall authentication.
config vpn certificate ca	
edit <ca_name>	
set auto-update-days	New field. Sets the number of days prior to expiry that the FortiGate unit requests an updated CA certificate.
set auto-update-days-warning	New field. Sets how many days before CA certificate expiry the FortiGate generates a warning message.
set scep-url	New field. Specifies the URL of the SCEP server.
config vpn certificate crl	
edit <crl_name>	
set update-interval	New field. Sets how frequently the FortiGate unit checks for an updated CRL.
config vpn certificate local	
edit <cert_name>	
set auto-regenerate-days	New field. Sets the number of days prior to expiry that the FortiGate unit requests an updated local certificate.
set auto-regenerate-days-warning	New field. Sets how many days before local certificate expiry the FortiGate generates a warning message.
set scep-password	New field. Specifies the password for the SCEP server.
set scep-url	New field. Specifies the URL of the SCEP server.

Command	Change
config vpn ipsec phase1-interface	
edit <gateway_name>	
set dhgrp	New option 14 to select DH Group 14.
set ike-version	New field. Selects IKEv1 or IKEv2.
set mode-cfg	New field. Enables IKE Configuration Method. The following new fields are available when mode-cfg is enabled: add-route, assign-ip, assign-ip-from, assign-ip-type, banner, domain, end-ip, mode-cfg-ip-version, ipv4-dns-server1, ipv6-dns-server1, ipv4-dns-server2, ipv6-dns-server2, ipv4-dns-server3, ipv6-dns-server3, ipv4-end-ip, ipv6-end-ip, ipv4-netmask, ipv4-split-include, ipv4-start-ip, ipv6-start-ip, ipv4-wins-server1, ipv4-wins-server2, ipv6-prefix, start-ip, unity-support
set proposal	New option sha256 for SHA256 digest.
config vpn ssl settings	
set force-two-factor-auth	New field. Requires PKI (peer) users to authenticate by password in addition to certificate authentication.
set force-utf8-login	New field. Causes UTF-8 encoding to be used on login page.
set deflate-compression-level set deflate-min-data-size	New fields. These tune the HTTP compression enabled with the new http-compression field.
set http-compression	New field. Enables HTTP compression between the FortiGate unit and the client browser.
set tunnel-startip set tunnel-endip	Fields removed. Address ranges are now defined as firewall addresses. See tunnel-ip-pools.
set tunnel-ip-pools	New field. Replaces tunnel-startip and tunnel-endip. Address ranges are defined as firewall addresses and selected by name.
config vpn ssl web bookmarks	Command removed. Bookmarks are now configured in the web portal using the Bookmark widget.
config vpn ssl web host-check-software	New command. Configures security applications to use in custom host checks.
config vpn ssl web portal	
edit <portal_name>	
set client-check set client-check-type	Fields removed. See host-check instead.
set host-check	New field. Selects type of host checking to perform.
set host-check-interval	New field. Selects
set host-check-policy	New field. Selects applications for custom host check.
set layout	Renamed to page-layout.
set limit-user-logins	New field. Limits each user to a single SSL VPN session.
set page-layout	Renamed from layout.
config widget	
set start-ip set end-ip	Fields removed. Address ranges are now defined as firewall addresses. See ip-pools.
set ip-pools	New field. Replaces start-ip and end-ip. Address ranges are defined as firewall addresses and selected by name.
set split-tunneling-routing-address	New field. Provides destination address information for client's routing table.

Command	Change
config vpn ssl web portal (continued)	
edit <portal_name>	
config bookmarks	
set sso	New field. Configures a Single Sign-On (SSO) bookmark.
config form-data	New subcommand. Configures credentials for static SSO bookmarks.
config wanopt iscsi	Command removed.
config wanopt settings	
set log-traffic {cifs ftp http mapi tcp}	New field. Enable WAN optimization and WAN optimization web caching traffic logging.
config web-proxy global	
set forward-proxy-auth	New field. Enable or disable configuring the explicit web proxy to forward proxy authentication headers.
set strict-web-check	New field. Enable or disable configuring the explicit web proxy to block web sites that send incorrect headers that do not conform to HTTP 1.1.
config webfilter block	Command removed. See config webfilter content.
config webfilter content	New command. Controls web content by blocking or exempting words, phrases, or patterns. This command includes some functionality of old config webfilter block and config webfilter exmword commands.
config webfilter content-header	New command. Filters web content according to the MIME content header.
config webfilter exmword	Command removed. See config webfilter content.
config webfilter ftgd-ovrd	
edit <override_int>	
set ip6	New field. Specifies the IPv6 IP address for which the override rule applies.
set scope	New option ip6 sets scope of override rule to ip6 setting.
config webfilter urlfilter	
edit <list_int>	
config entries	
edit <url_str>	
set type	New URL filter type option wildcard.
config wireless-controller ...	New commands for configuring the wireless controller feature.
execute log delete-filtered	Command removed.
execute log filter dump	Renamed from execute log filter list.
execute log filter ha-member	New command. Selects logs from the specified HA cluster member.
execute log filter lines-per-view	Renamed to execute log filter view-lines.
execute log filter list	Renamed to execute log filter dump.
execute log filter view-lines	Renamed from execute log filter lines-per-view.
execute vpn sslvpn del-all	New command. Deletes all SSL VPN connections in this VDOM.
execute vpn sslvpn list	New command. Lists current SSL VPN tunnel connections.
execute wireless-controller delete-wtp-image	New command. Deletes all FortiWiFi access point firmware images stored on the FortiGate unit.

Command	Change
execute wireless-controller reset-wtp	New command. Reset a physical access point (WTP).
execute wireless-controller restart-daemon	New command. Restarts the wireless-controller.
execute wireless-controller upload-wtp-image	New command. Uploads a FortiWiFi firmware image to the FortiGate unit.
get endpoint-control app-detect predefined-category status	New command. Retrieves information about predefined application detection categories.
get endpoint-control app-detect predefined-group status	New command. Retrieves information about predefined application detection groups.
get endpoint-control app-detect predefined-signature status	New command. Retrieves information about predefined application detection signatures.
get endpoint-control app-detect predefined-vendor status	New command. Retrieves information about predefined application detection vendors.
get report database schema	New command. Displays the SQL report database schema.
get router info6 bgp	New command. Displays information about the BGP IPv6 configuration.
get router info6 ospf	New command. Displays information about the OSPF IPv6 configuration.
get router info6 protocols	New command. Displays information about the configuration of all IPv6 dynamic routing protocols.
get router info6 rip	New command. Displays information about the RIPng configuration.
get wireless-controller scan	New command. Displays the list of detected access points.
get wireless-controller status	New command. Lists the physical AP (WTP) firmware images stored on the wireless-controller.

Using the CLI

The command line interface (CLI) is an alternative to the web-based manager.

Both can be used to configure the FortiGate unit. However, to perform the configuration, in the web-based manager, you would use buttons, icons, and forms, while, in the CLI, you would either type lines of text that are commands, or upload batches of commands from a text file, like a configuration script.

If you are new to Fortinet products, or if you are new to the CLI, this section can help you to become familiar.

This section contains the following topics:

Connecting to the CLI

You can access the CLI in two ways:

- **Locally** — Connect your computer directly to the FortiGate unit's console port.
- **Through the network** — Connect your computer through any network attached to one of the FortiGate unit's network ports. The network interface must have enabled Telnet or SSH administrative access if you will connect using an SSH/Telnet client, or HTTP/HTTPS administrative access if you will connect using the *CLI Console* widget in the web-based manager.

Local access is required in some cases.

- If you are installing your FortiGate unit for the first time and it is not yet configured to connect to your network, unless you reconfigure your computer's network settings for a peer connection, you may only be able to connect to the CLI using a local serial console connection. See the *FortiGate Install Guide*.
- Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until ***after*** the boot process has completed, and therefore local CLI access is the only viable option.

Before you can access the CLI through the network, you usually must enable SSH and/or Telnet on the network interface through which you will access the CLI.

This section includes the following:

Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiGate unit, using its DB-9 or RJ-45 console port.

Requirements

- a computer with an available serial communications (COM) port
- the RJ-45-to-DB-9 or null modem cable included in your FortiGate package
- terminal emulation software such as HyperTerminal for Microsoft Windows

Note: The following procedure describes connection using Microsoft HyperTerminal software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiGate unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start HyperTerminal.
3. On *Connection Description*, enter a *Name* for the connection, and select *OK*.
4. On *Connect To*, from *Connect using*, select the communications (COM) port where you connected the FortiGate unit.
5. Select *OK*.
6. Select the following *Port* settings and select *OK*.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7. Press Enter to connect to the CLI.

   The login prompt appears.
8. Type a valid administrator account name (such as `admin`) and press Enter.
9. Type the password for that administrator account and press Enter. (In its default state, there is no password for the `admin` account.)

   The CLI displays the following text:

   ```
   Welcome!
   Type ? to list available commands.
   ```

   You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 32.

Enabling access to the CLI through the network (SSH or Telnet)

SSH or Telnet access to the CLI is formed by connecting your computer to the FortiGate unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

Note: If you do not want to use an SSH/Telnet client and you have access to the web-based manager, you can alternatively access the CLI through the network using the *CLI Console* widget in the web-based manager. For details, see the *FortiGate Administration Guide*.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is ***not*** connected directly or through a switch, you must also configure the FortiGate unit with a static route to a router that can forward packets from the FortiGate unit to your computer.

You can do this using either:

- a local console connection (see the following procedure)
- the web-based manager (see the *FortiGate Install Guide* or the *FortiGate Administration Guide*)

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as HyperTerminal for Microsoft Windows
- the RJ-45-to-DB-9 or null modem cable included in your FortiGate package
- a crossover or straight-through network cable
- prior configuration of the operating mode, network interface, and static route (for details, see the *FortiGate Install Guide*)

To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiGate unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiGate unit.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI. For details, see "Connecting to the CLI using a local console" on page 32.
4. Enter the following command:

```
config system interface
  edit <interface_str>
    set allowaccess <protocols_list>
    next
  end
```

where:

- `<interface_str>` is the name of the network interface associated with the physical network port and containing its number, such as `port1`
- `<protocols_list>` is the complete, space-delimited list of permitted administrative access protocols, such as `https ssh telnet`

For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on `port1`:

```
set system interface port1 config allowaccess ssh telnet
```

Caution: Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

5 To confirm the configuration, enter the command to display the network interface's settings.

```
get system interface <interface_str>
```

The CLI displays the settings, including the allowed administrative access protocols, for the network interfaces.

To connect to the CLI through the network interface, see "Connecting to the CLI using SSH" on page 34 or "Connecting to the CLI using Telnet" on page 35.

Connecting to the CLI using SSH

Once the FortiGate unit is configured to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI.

Note: FortiGate units support 3DES and Blowfish encryption algorithms for SSH.

Before you can connect to the CLI using SSH, you must first configure a network interface to accept SSH connections. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 32.

Note: The following procedure uses PuTTY. Steps may vary with other SSH clients.

To connect to the CLI using SSH

1 On your management computer, start an SSH client.

2 In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled SSH administrative access.

3 In *Port*, type `22`.

4 From *Connection type*, select *SSH*.

5 Select *Open*.

The SSH client connects to the FortiGate unit.

The SSH client may display a warning if this is the first time you are connecting to the FortiGate unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiGate unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiGate unit with no network hosts between them, this is normal.

6 Click *Yes* to verify the fingerprint and accept the FortiGate unit's SSH key. You will not be able to log in until you have accepted the key.

The CLI displays a login prompt.

7 Type a valid administrator account name (such as `admin`) and press Enter.

Note: You can alternatively log in using an SSH key. For details, see "system admin" on page 385.

8 Type the password for this administrator account and press Enter.

Note: If three incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The FortiGate unit displays a command prompt (its host name followed by a #).

You can now enter CLI commands.

Connecting to the CLI using Telnet

Once the FortiGate unit is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.

Caution: Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Before you can connect to the CLI using Telnet, you must first configure a network interface to accept SSH connections. For details, see "Enabling access to the CLI through the network (SSH or Telnet)" on page 32.

To connect to the CLI using Telnet

1. On your management computer, start a Telnet client.
2. Connect to a FortiGate network interface on which you have enabled Telnet.
3. Type a valid administrator account name (such as `admin`) and press Enter.
4. Type the password for this administrator account and press Enter.

Note: If three incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The FortiGate unit displays a command prompt (its host name followed by a #).

You can now enter CLI commands.

Command syntax

When entering a command, the command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Fortinet documentation uses the following conventions to describe valid command syntax

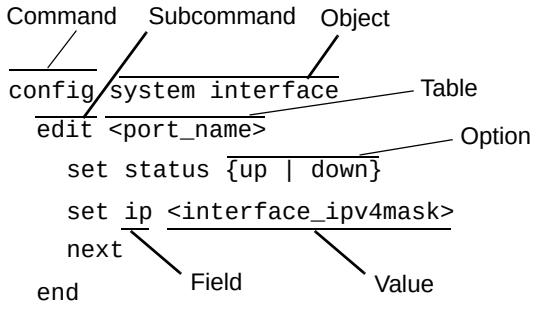
Terminology

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

To describe the function of each word in the command line, especially if that nature has changed between firmware versions, Fortinet uses terms with the following definitions.

Figure 1: Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiGate unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line. Exceptions include multi-line command lines, which can be entered using an escape sequence. (See "Shortcuts and key commands" on page 45.)

  Valid command lines must be unambiguous if abbreviated. (See "Command abbreviation" on page 45.) Optional words or other command line permutations are indicated by syntax notation. (See "Notation" on page 37.)

Note: This CLI Reference is organized alphabetically by object for the `config` command, and by the name of the command for remaining top-level commands.

- **sub-command** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nested commands. (See "Indentation" on page 37.)

  Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope. (See "Sub-commands" on page 39.)
- **object** — A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them. (See "Notation" on page 37.)
- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiGate unit will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation. (See "Notation" on page 37.)
- **option** — A kind of value that must be one or more words from of a fixed set of options. (See "Notation" on page 37.)

Indentation

Indentation indicates levels of nested commands, which indicate what other sub-commands are available from within the scope.

For example, the `edit` sub-command is available only within a command that affects tables, and the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
    next
  end
```

For information about available sub-commands, see "Sub-commands" on page 39.

Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Table 2: Command syntax notation

Convention	Description

Square brackets `[ ]`	A non-required word or series of words. For example:
	`[verbose {1 | 2 | 3}]`
	indicates that you may either omit or type both the `verbose` word and its accompanying option, such as:
	`verbose 3`

Table 2: Command syntax notation

Angle brackets < >		A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route. • `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`. • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>`: An email address, such as `admin@mail.example.com`. • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`. • `<xxx_ipv4range>`: A hyphen (`-`)-delimited inclusive range of IPv4 addresses, such as `192.168.1.1-192.168.1.255`. • `<xxx_ipv6>`: A colon(`:`)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`. • `<xxx_v6mask>`: An IPv6 netmask, such as `/96`. • `<xxx_ipv6mask>`: A dotted decimal IPv6 address and netmask separated by a space. • `<xxx_str>`: A string of characters that is ***not*** another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See “Special characters” on page 46. • `<xxx_int>`: An integer number that is ***not*** another data type, such as `15` for the number of minutes.
Curly braces { }		A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
	Options delimited by vertical bars |	Mutually exclusive options. For example: `{enable | disable}` indicates that you must enter either `enable` or `disable`, but must not enter both.

	Options delimited by spaces	Non-mutually exclusive options. For example:
		`{http https ping snmp ssh telnet}`
		indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:
		`ping https ssh`
		Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type:
		`ping https snmp ssh`
		If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Sub-commands

Once you have connected to the CLI, you can enter commands.

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

Sub-commands are available from within the scope of some commands.When you enter a sub-command level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command.

For example, the `edit` sub-command is available only within a command that affects tables; the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
    next
  end
```

Note: Sub-command scope is indicated in this CLI Reference by indentation. See "Indentation" on page 37.

Available sub-commands vary by command.From a command prompt within `config`, two types of sub-commands might become available:

- commands affecting fields
- commands affecting tables

Note: Syntax examples for each top-level command in this CLI Reference do not show all available sub-commands. However, when nested scope is demonstrated, you should assume that sub-commands applicable for that level of scope are available.

Table 3: Commands for tables

delete <table>	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `first-name` and `email-address`. `delete` is only available within objects containing tables.
edit <table>	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive sub-command: further sub-commands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables.
end	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values. For more information on `get` commands, see "get" on page 767.
purge	Remove all tables in the current object. For example, in `config forensic user`, you could type `get` to see the list of user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiGate unit before performing a `purge`. `purge` cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see execute backup. **Caution:** Do not purge `system interface` or `system admin` tables. `purge` does not provide default tables. This can result in being unable to connect or log in, requiring the FortiGate unit to be formatted and restored.
rename <table> to <table>	Rename a table. For example, in `config system admin`, you could rename `admin3` to `fwadmin` by typing `rename admin3 to fwadmin`. `rename` is only available within objects containing tables.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1)#
```

Table 4: Commands for fields

abort	Exit both the `edit` and/or `config` commands without saving the fields.
end	Save the changes made to the current table or object fields, and exit the `config` command. (To exit without saving, use `abort` instead.)
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
next	Save the changes you have made in the current table's fields, and exit the `edit` command to the object prompt. (To save and exit completely to the root prompt, use `end` instead.) `next` is useful when you want to create or edit several tables in the same object, without leaving and re-entering the `config` command each time. `next` is only available from a table prompt; it is not available from an object prompt.
set <field> <value>	Set a field's value. For example, in `config system admin`, after typing `edit admin`, you could type `set password newpass` to change the password of the `admin` administrator to `newpass`. **Note:** When using `set` to change a field containing a space-delimited list, type the whole new list. For example, `set <field> <new-value>` will replace the list with the `<new-value>` rather than appending `<new-value>` to the list.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unset <field>	Reset the table or object's fields to default values. For example, in `config system admin`, after typing `edit admin`, typing `unset password` resets the password of the `admin` administrator account to the default (in this case, no password).

Example of field commands

From within the `admin_1` table, you might enter:

```
set password my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `password` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

Permissions

Depending on the account that you use to log in to the FortiGate unit, you may not have complete access to all CLI commands.

Access profiles control which CLI commands an administrator account can access.

Access profiles assign either read, write, or no access to each area of the FortiGate software. To view configurations, you must have read access. To make changes, you must have write access. For more information on configuring an access profile that administrator accounts can use, see "system accprofile" on page 382.

Table 5: Areas of control in access profiles

Access control area name		Grants access to (For each `config` command, there is an equivalent get/show command, unless otherwise noted. `config` access requires write permission. `get`/`show` access requires read permission.)
In the web-based manager	**In the CLI**	

Admin Users	`admingrp`	*System > Admin*
		`config system admin`
		`config system accprofile`

Auth Users	`authgrp`	*User*
		`config imp2p aim-user`
		`config imp2p icq-user`
		`config imp2p msn-user`
		`config imp2p yahoo-user`
		`config user`

Endpoint NAC	`endpoint-control-grp`	*Endpoint NAC* `config endpoint-control`

Firewall Configuration	`fwgrp`	*Firewall*
		`config firewall`
		`config gui topology`
		`execute fsae refresh`

FortiGuard Update	`updategrp`	*System > Maintenance > FortiGuard*
		`config system autoupdate`
		`execute update-ase`
		`execute update-av`
		`execute update-ips`
		`execute update-now`

Log & Report	`loggrp`	*Log&Report*
		`cconfig alertemail`
		`config log`
		`config system alertemail`
		`config system fortianalyzer1/2/3`
		`execute formatlogdisk`
		`execute fortiguard-log`
		`execute log`

Maintenance	`mntgrp`	*System > Maintenance*
		`diagnose sys ...`
		`execute backup ...`
		`execute batch`
		`execute central-mgmt`
		`execute factoryreset`
		`execute reboot`
		`execute restore`
		`execute shutdown`
		`execute usb-disk`

Network Configuration	`netgrp`	*System > Network > Interface* `config system interface`

Table 5: Areas of control in access profiles

Router Configuration	`routegrp`	*Router*
		`config router ...`
		`execute mrouter`
		`execute router`

System Configuration	`sysgrp`	*System* > *Status* (all), *System* > *Network* > *Options*, *System* > *Network* > *DNS Database*, *System* > *Config* (all), *System* > *Admin* > *Central Management*, *System* > *Admin* > *Settings*, *Wireless Controller*
		`config gui console`
		`config system auto-install`, `bug report`, `central-management`, `console`, `dns`, `dns-database`, `fips-cc`, `fortiguard`, `fortiguard-log`, `global`, `ha`, `ipv6-tunnel`, `modem`, `ntp`, `password-policy`, `replacemsg`, `session-helper`, `session-sync`, `session-ttl`, `settings`, `sit-tunnel`, `snmp`, `switch-interface`, `tos-based-priority`, `wccp`
		`config wireless-controller ...`
		`execute cfg`, `cli`, `date`, `disconnect-admin-session`, `enter`, `factoryreset`, `fortiguard-log`, `ha`, `modem`, `ping`, `ping-options`, `ping6`, `ping6-options`, `reboot`, `send-fds-statistics`, `set-next-reboot`, `shutdown`, `ssh`, `telnet`, `time`, `traceroute`
		`get gui console`
		`get ipsec tunnel`
		`get system central-mgmt`, `cmdb`, `fdp-fortianalyzer`, `fortianalyzer-connectivity`, `fortiguard-log-service`, `fortiguard-service`, `info`, `performance`, `session`
		`get wireless-controller`

UTM Configuration	`utmgrp`	*UTM*
		`config antivirus`
		`config application`
		`config imp2p old-version`
		`config imp2p policy`
		`config ips`
		`config spamfilter`
		`config webfilter`

VPN Configuration	`vpngrp`	*VPN*
		`config vpn`
		`execute vpn`

Unlike other administrator accounts, the administrator account named `admin` exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiGate configuration options, including viewing and changing *all* other administrator accounts. Its name and permissions cannot be changed. It is the only administrator account that can reset another administrator's password without being required to enter that administrator's existing password.

Caution: Set a strong password for the `admin` administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiGate unit.

For complete access to all commands, you must log in with the administrator account named `admin`.

Tips and tricks

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

This section includes:

- Help
- Shortcuts and key commands
- Command abbreviation
- Environment variables
- Special characters
- Language support & regular expressions
- Screen paging
- Baud rate
- Editing the configuration file on an external host

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Table 6: Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Complete the word with the next available match. Press the key multiple times to cycle through available matches.	Tab
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.	Ctrl + C
Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy st`.

Environment variables

The CLI supports the following environment variables. Variable names are case-sensitive.

$USERFROM	The management access type (`ssh`, `telnet`, `jsconsole` for the *CLI Console* widget in the web-based manager, and so on) and the IP address of the administrator that configured the item.
$USERNAME	The account name of the administrator that configured the item.
$SerialNum	The serial number of the FortiGate unit.

For example, the FortiGate unit's host name can be set to its serial number.

```
config system global
  set hostname $SerialNum
end
```

As another example, you could log in as `admin1`, then configure a restricted secondary administrator account for yourself named `admin2`, whose `first-name` is `admin1` to indicate that it is another of your accounts:

```
config system admin
  edit admin2
    set first-name $USERNAME
```

Special characters

The characters <, >, (,), #, ', and “ are not permitted in most CLI fields. These characters are special characters, sometimes also called reserved characters.

You may be able to enter a special character as part of a string’s value by using a special command, enclosing it in quotes, or preceding it with an escape sequence — in this case, a backslash (\ ) character.

Table 7: Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	Enclose the string in quotation marks: `"Security Administrator"`. Enclose the string in single quotes: `'Security Administrator'`. Precede the space with a backslash: `Security\ Administrator`.
' (to be interpreted as part of a string value, not to end the string)	\'
" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Language support & regular expressions

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice.

For example, the host name must not contain special characters, and so the web-based manager and CLI will not accept most symbols and other non-ASCII encoded characters as input when configuring the host name. This means that languages other than English often are not supported. However, some configuration items, such as names and comments, may be able to use the language of your choice.

To use other languages in those cases, you must use the correct encoding.

Input is stored using Unicode UTF-8 encoding, but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, your configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using another encoding, or if an HTTP client sends a request in an encoding other than UTF-8, matches may not be what you expect.

For example, with Shift-JIS, backslashes (\ ) could be inadvertently interpreted as yen symbols (¥) and vice versa. A regular expression intended to match HTTP requests containing money values with a yen symbol therefore may not work it if the symbol is entered using the wrong encoding.

For best results, you should:

- use UTF-8 encoding, or
- use only the characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are also encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS and other encodings, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients

Note: HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary by the client's operating system or input language. If you cannot predict the client's encoding, you may only be able to match any parts of the request that are in English, because regardless of the encoding, the values for English characters tend to be encoded identically. For example, English words may be legible regardless of interpreting a web page as either ISO 8859-1 or as GB2312, whereas simplified Chinese characters might only be legible if the page is interpreted as GB2312.

In order to configure your FortiGate unit using other encodings, you may need to switch language settings on your management computer, including for your web browser or Telnet/SSH client. For instructions on how to configure your management computer's operating system language, locale, or input method, see its documentation.

Note: If you choose to configure parts of the FortiGate unit using non-ASCII characters, verify that all systems interacting with the FortiGate unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web-based manager and your web browser or Telnet/SSH client while you work.

Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the web-based manager or CLI. Exceptions include items such as regular expressions that you may have configured using other encodings in order to match the encoding of HTTP requests that the FortiGate unit receives.

To enter non-ASCII characters in the CLI Console widget

1. On your management computer, start your web browser and go to the URL for the FortiGate unit's web-based manager.
2. Configure your web browser to interpret the page as UTF-8 encoded.
3. Log in to the FortiGate unit.
4. Go to *System* > *Status* > *Status*.
5. In title bar of the *CLI Console* widget, click *Edit*.

   The *Console Preferences* window appears in a pop-up window.

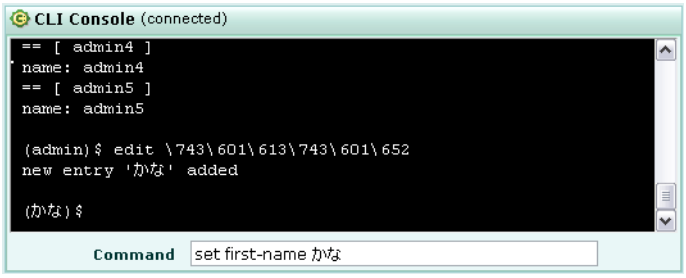
6 Enable *Use external command input box*.

7 Click *OK*.

The *Command* field appears below the usual input and display area of the *CLI Console* widget.

8 In *Command*, type a command.

Figure 2: Entering encoded characters *(CLI Console* widget)



9 Press Enter.

In the display area, the *CLI Console* widget displays your previous command interpreted into its character code equivalent, such as:

```
edit \743\601\613\743\601\652
```

and the command's output.

To enter non-ASCII characters in a Telnet/SSH client

1 On your management computer, start your Telnet or SSH client.

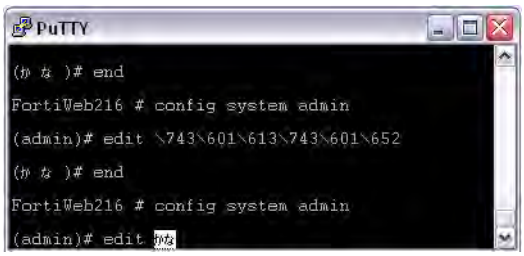
2 Configure your Telnet or SSH client to send and receive characters using UTF-8 encoding.

Support for sending and receiving international characters varies by each Telnet/SSH client. Consult the documentation for your Telnet/SSH client.

3 Log in to the FortiGate unit.

4 At the command prompt, type your command and press Enter.

Figure 3: Entering encoded characters (PuTTY)



You may need to surround words that use encoded characters with single quotes (').

Depending on your Telnet/SSH client's support for your language's input methods and for sending international characters, you may need to interpret them into character codes before pressing Enter.

For example, you might need to enter:

```
edit '\743\601\613\743\601\652'
```

5 The CLI displays your previous command and its output.

Screen paging

You can configure the CLI to, when displaying multiple pages' worth of output, pause after displaying each page's worth of text. When the display pauses, the last line displays `--More--`. You can then either:

- Press the spacebar to display the next page.
- Type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause when the screen is full:

```
config system console
  set output more
end
```

For more information, see "system console" on page 408.

Baud rate

You can change the default baud rate of the local console connection. For more information, see "system console" on page 408.

Editing the configuration file on an external host

You can edit the FortiGate configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiGate unit.

Editing the configuration on an external host can be time-saving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

To edit the configuration on your computer

1 Use execute backup to download the configuration file to a TFTP server, such as your management computer.

2 Edit the configuration file using a plain text editor that supports Unix-style line endings.

Caution: Do not edit the first line. The first line(s) of the configuration file (preceded by a # character) contains information about the firmware version and FortiGate model. If you change the model number, the FortiGate unit will reject the configuration file when you attempt to restore it.

3 Use execute restore to upload the modified configuration file back to the FortiGate unit.

The FortiGate unit downloads the configuration file and checks that the model information is correct. If it is, the FortiGate unit loads the configuration file and checks each command for errors.If a command is invalid, the FortiGate unit ignores the command. If the configuration file is valid, the FortiGate unit restarts and loads the new configuration.

Using Perl regular expressions

Some FortiGate features, such as spam filtering and web content filtering can use either wildcards or Perl regular expressions.

See http://perldoc.perl.org/perlretut.html for detailed information about using Perl regular expressions.

Some differences between regular expression and wildcard pattern matching

In Perl regular expressions, '.' character refers to any single character. It is similar to the '?' character in wildcard pattern matching. As a result:

- `fortinet.com` not only matches `fortinet.com` but also matches `fortinetacom`, `fortinetbcom`, `fortinetccom` and so on.

To match a special character such as '.' and '*', regular expressions use the '\' escape character. For example:

- To match `fortinet.com`, the regular expression should be `fortinet\.com`.

In Perl regular expressions, '*' means match 0 or more times of the character before it, not 0 or more times of any character. For example:

- `forti*\.com` matches `fortiiii.com` but does not match `fortinet.com`.

To match any character 0 or more times, use '.*' where '.' means any character and the '*' means 0 or more times. For example:

- the wildcard match pattern `forti*.com` is equivalent to the regular expression `forti.*\.com`.

Word boundary

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression "test" not only matches the word "test" but also matches any word that contains the word "test" such as "atest", "mytest", "testimony", "atestb". The notation "\b" specifies the word boundary. To match exactly the word "test", the expression should be `\btest\b`.

Case sensitivity

Regular expression pattern matching is case sensitive in the Web and Spam filters. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of "bad language" regardless of case.

Table 8: Perl regular expression examples

Expression	Matches
abc	abc (that exact character sequence, but anywhere in the string)
^abc	abc at the beginning of the string
abc$	abc at the end of the string
a|b	either of a and b
^abc|abc$	the string abc at the beginning or at the end of the string
ab{2,4}c	an a followed by two, three or four b's followed by a c
ab{2,}c	an a followed by at least two b's followed by a c
ab*c	an a followed by any number (zero or more) of b's followed by a c
ab+c	an a followed by one or more b's followed by a c
ab?c	an a followed by an optional b followed by a c; that is, either abc or ac
a.c	an a followed by any single character (not newline) followed by a c
a\.c	a.c exactly
[abc]	any one of a, b and c
[Aa]bc	either of Abc and abc
[abc]+	any (nonempty) string of a's, b's and c's (such as a, abba, acbabcacaa)
[^abc]+	any (nonempty) string which does not contain any of a, b and c (such as defg)
\d\d	any two decimal digits, such as 42; same as \d{2}
/i	makes the pattern case insensitive. For example, `/bad language/i` blocks any instance of “bad language” regardless of case.
\w+	a "word": a nonempty sequence of alphanumeric characters and low lines (underscores), such as foo and 12bar8 and foo_1
100\s*mk	the strings 100 and mk optionally separated by any amount of white space (spaces, tabs, newlines)
abc\b	abc when followed by a word boundary (e.g. in abc! but not in abcd)
perl\B	perl when not followed by a word boundary (e.g. in perlert but not in perl stuff)
\x	tells the regular expression parser to ignore white space that is neither backslashed nor within a character class. You can use this to break up your regular expression into (slightly) more readable parts.

Working with virtual domains

By default, the FortiGate unit has one virtual domain (root) and one administrator (admin) with unrestricted access to the system configuration. If you enable virtual domain configuration, the super admin account can also:

- Use the `vdom` command to create and configure additional virtual domains.
- Use the `global` command to create and assign administrators to each virtual domain.
- Use the `global` command to configure features that apply to all virtual domains.

This section contains the following topics:

Enabling virtual domain configuration

The administrators with the super_admin profile can enable virtual domain configuration through either the web-based manager or the CLI. In the CLI, use the following command:

```
config system global
  set vdom-admin enable
end
```

Log off and then log on again with a super_admin admin account. By default, there is no password for the default admin account.

Accessing commands in virtual domain configuration

When you log in as admin with virtual domain configuration enabled, you have only four top-level commands:

`config global`	Enter `config global` to access global commands. In the `global` shell, you can execute commands that affect all virtual domains, such as `config system autoupdate`. For a list of the global commands, see "global" on page 59.
`config vdom`	Enter `config vdom` to access VDOM-specific commands. In the `vdom` shell, use the `edit <vdom_name>` command to create a new VDOM or to edit the configuration of an existing VDOM. In the `<vdom_name>` shell, you can execute commands to configure options that apply only within the VDOM, such as `config firewall policy`. For a list of VDOM-specific commands, see "vdom" on page 62. When you have finished, enter `next` to edit another vdom, or `end`.
`get system status`	System status. For more information, see "vdom-link" on page 533.
`exit`	Log off.

Creating and configuring VDOMs

When virtual domain configuration is enabled, admin has full access to the global FortiGate unit configuration and to the configuration of each VDOM. All of the commands described in this Reference are available to admin, but they are accessed through a special top-level command shell.

Creating a VDOM

You create a new VDOM using the `config vdom` command. For example, to create a new VDOM called vdomain2, you enter the following:

```
config vdom
  edit vdomain2
end
```

This creates a new VDOM operating in NAT/Route mode. You can have up to 10 VDOMs on your FortiGate unit by default.

For this VDOM to be useful, you need to assign interfaces or VLAN subinterfaces to it.

Assigning interfaces to a VDOM

By default, all interfaces belong to the root domain. You can reassign an interface or VLAN subinterface to another VDOM if the interface is not already used in a VDOM-specific configuration such as a firewall policy. Interfaces are part of the global configuration of the FortiGate unit, so only the admin account can configure interfaces.

For example, to assign port3 and port4 to vdomain2, log on as admin and enter the following commands:

```
config global
  config system interface
    edit port3
      set vdom vdomain2
    next
    edit port4
      set vdom vdomain2
    end
  end
```

Setting VDOM operating mode

When you create a VDOM, its default operating mode is NAT/Route. You can change the operating mode of each VDOM independently. When viewing a list of interfaces that are in different VDOMs and different operating modes, fields that are not available for some interfaces will display a “-”.

Changing to Transparent mode

When you change the operating mode of a VDOM from NAT/Route to Transparent mode, you must specify the management IP address and the default gateway IP address. The following example shows how to change vdomain2 to Transparent mode. The management IP address is 192.168.10.100, and the default gateway is 192.168.10.1:

```
config vdom
  edit vdomain3
    config system settings
       set opmode transparent
       set manageip 192.168.10.100 255.255.255.0
       set gateway 192.168.10.1
    end
```

For more information, see “system settings” on page 517.

Changing back to NAT/Route mode

If you change a Transparent mode VDOM back to NAT/Route mode, you must specify which interface you will use for administrative access and the IP address for that interface. This ensures that administrative access is configured on the interface. You must also specify the default gateway IP address and the interface that connects to the gateway. For example,

```
config vdom
  edit vdomain3
    config system settings
      set opmode nat
    end
    config system interface
    edit port1
      set ip 192.168.10.100 255.255.255.0
    end
```

For more information, see "system settings" on page 517.

Configuring inter-VDOM routing

By default, VDOMs are independent of each other and to communicate they need to use physical interfaces that are externally connected. By using the `vdom-link` command that was added in FortiOS v3.0, this connection can be moved inside the FortiGate unit, freeing up the physical interfaces. This feature also allows you to determine the level of inter-VDOM routing you want - only 2 VDOMs inter-connected, or interconnect all VDOMs. The `vdom-link` command creates virtual interfaces, so you have access to all the security available to physical interface connections. These internal interfaces have the added bonus of being faster the physical interfaces unless the CPU load is very heavy. As of FortiOS v3.0 MR3, BGP is supported over inter-VDOM links.

A packet can pass through an inter-VDOM link a maximum of three times. This is to prevent a loop. When traffic is encrypted or decrypted it changes the content of the packets and this resets the inter-VDOM counter. However using IPIP or GRE tunnels do not reset the counter.

VDOM-links can also be configured through the web-based management interface. For more information, see the FortiGate Administration Guide.

In this example you already have configured two VDOMs called v1 and v2. You want to set up a link between them. The following command creates the VDOM link called v12_link. Once you have the link in place, you need to bind the two ends of the link to the VDOMs it will be connecting. Then you are free to apply firewall policies or other security measures.

```
config global
config system vdom-link
  edit v12_link
end
config system interface
  edit v12_link0
    set vdom v1
  next
  edit v12_link1
    set vdom v2
  next
end
```

Note: When you are naming VDOM links you are limited to 8 characters for the base name. In the example below the link name v12_link that is used is correct, but a link name of v12_verylongname is too long.

To remove the vdom-link, delete the vdom-link. You will not be able to delete the ends of the vdom-link by themselves. To delete the above set up, enter:

```
config global
config system vdom-link
  delete v12_link
end
```

Note: In an HA setup with virtual clusters, inter-VDOM routing must be entirely within one cluster. You cannot create links between virtual clusters, and you cannot move a VDOM that is linked into another virtual cluster. In HA mode, with multiple vclusters when you create the vdom-link in system vdom-link there is an option to set which vcluster the link will be in.

Before inter-VDOM routing, VDOMs were completely separate entities. Now, many new configurations are available such as a service provider configuration (a number of VDOMS that go through one main VDOM to access the internet) or a mesh configuration (where some or all VDOMs are connected to some or all other VDOMs). These configurations are discussed in-depth in the FortiGate VLANs and VDOMs Guide.

Changing the management VDOM

All management traffic leaves the FortiGate unit through the management VDOM. Management traffic includes all external logging, remote management, and other Fortinet services. By default the management VDOM is root. You can change this to another VDOM so that the traffic will leave your FortiGate unit over the new VDOM.

You cannot change the management VDOM if any administrators are using RADIUS authentication.

If you want to change the management VDOM to vdomain2, you enter:

```
config global
config system global
  set management-vdom vdomain2
end
```

Creating VDOM administrators

The super_admin admin accounts can create regular administrators and assign them to VDOMs. The `system admin` command, when accessed by admin, includes a VDOM assignment.

For example, to create an administrator, admin2, for VDOM vdomain2 with the default profile prof_admin, you enter:

```
config global
  config system admin
  edit admin2
    set accprofile prof_admin
    set password hardtoguess
    set vdom vdomain2
  end
```

The admin2 administrator account can only access the vdomain2 VDOM and can connect only through an interface that belongs to that VDOM. The VDOM administrator can access only VDOM-specific commands, not global commands.

Troubleshooting ARP traffic on VDOMs

Address Resolution Protocol (ARP) traffic is vital to communication on a network and is enabled on FortiGate interfaces by default. Normally you want ARP packets to pass through the FortiGate unit, especially if it is sitting between a client and a server or between a client and a router.

Duplicate ARP packets

ARP traffic can cause problems, especially in Transparent mode where ARP packets arriving on one interface are sent to all other interfaces, including VLAN subinterfaces. Some Layer 2 switches become unstable when they detect the same MAC address originating on more than one switch interface or from more than one VLAN. This instability can occur if the Layer 2 switch does not maintain separate MAC address tables for each VLAN. Unstable switches may reset causing network traffic to slow down.

Multiple VDOMs solution

One solution is to configure multiple VDOMs on the FortiGate unit, one for each VLAN. This means one inbound and one outbound VLAN interface in each virtual domain. ARP packets are not forwarded between VDOMs.

By default, physical interfaces are in the root domain. Do not configure any of your VLANs in the root domain.

As a result of this VDOM configuration, the switches do not receive multiple ARP packets with the same source MAC but different VLAN IDs, and the instability does not occur.

Forward-domain solution

You may run into problems using the multiple VDOMs solution. It is possible that you have more VLANs than licensed VDOMs, not enough physical interfaces or your configuration may work better by grouping some VLANs together. In these situations the separate VDOMs solution may not work for you.

In these cases, the solution is to use the forward-domain <collision_group_number> command. This command tags VLAN traffic as belonging to a particular forward-domain collision group, and only VLANs tagged as part of that collision group receive that traffic. By default ports and VLANs are part of forward-domain collision group 0. For more information, see the FortiGate VLANs and VDOMs Guide.

There are many benefits for this solution from reduced administration, to using fewer physical interfaces to being able to allowing you more flexible network solutions.

In the following example, forward-domain collision group 340 includes VLAN 340 traffic on Port1 and untagged traffic on Port2. Forward-domain collision group 341 includes VLAN 341 traffic on Port1 and untagged traffic on Port3. All other ports are part of forward-domain collision group 0 by default.

These are the CLI commands to accomplish this setup.

```
config system interface
  edit “port1”
  next
  edit "port2"
    set forward_domain 340
  next
  edit “port3”
    set forward_domain 341
  next
  edit "port1-340"
    set forward_domain 340
    set interface "port1"
    set vlanid 340
  next
```

```
    edit "port1-341"
      set forward_domain 341
      set interface "port1"
      set vlanid 341
    next
  end
```

There is a more detailed discussion of this issue in the Asymmetric Routing and Other FortiGate Layer-2 Installation Issues technical note.

global

From a super_admin profile account, use this command to configure features that apply to the complete FortiGate unit including all virtual domains. Virtual domain configuration (vdom-admin) must be enabled first. For more information, see “system global” on page 423.

Syntax

This command syntax shows how you access the commands within config global. For information on these commands, refer to the relevant sections in this Reference. If there are multiple versions of the same command with a “2” or “3” added, the additional commands are not listed but fall under the unnumbered command of the same name.

```
config global
  config antivirus ...
  config application
  config firewall service
  config firewall ssl
  config gui console
  config ips ...
  config log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
  config log fortiguard setting
  config log memory setting
  config log memory global-setting
  config log {syslogd | syslogd2 | syslogd3} setting
  config log webtrends setting
  config spamfilter ...
  config system accprofile
  config system admin
  config system alertemail
  config system auto-install
  config system amc
  config system autoupdate clientoverride
  config system autoupdate override
  config system autoupdate push-update
  config system autoupdate schedule
  config system autoupdate tunneling
  config system bug-report
  config system central-management
  config system console
  config system dns
  config system fips-cc
  config system fortiguard
  conifg system fortiguard-log
  config system global
  config system ha
  config system interface
  config system npu
  config system ntp
  config system replacemsg admin
  config system replacemsg alertmail
  config system replacemsg auth
  config system replacemsg ec
  config system replacemsg fortiguard-wf
  config system replacemsg ftp
```

```
config system replacemsg http
config system replacemsg im
config system replacemsg mail
config system replacemsg nac-quar
config system replacemsg nntp
config system replacemsg spam
config system replacemsg sslvpn
config system session-helper
config system session-sync
config system snmp community
config system snmp sysinfo
config system switch-interface
conifg system tos-based-priority
config system vdom-link
config system vdom-property
config vpn certificate ca
config vpn certificate crl
config vpn certificate local
config vpn certificate remote
config webfilter fortiguard
execute backup
execute batch
execute central-mgmt
execute cfg reload
execute cfg save
execute cli check-template-status
execute cli status-msg-only
execute date
execute disconnect-admin-session
execute enter
execute factoryreset
execute formatlogdisk
execute fortiguard-log update
execute ha disconnect
execute ha manage
execute ha synchronize
execute log delete-all
execute log delete-rolled
execute log display
execute log filter
execute log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
execute log list
execute log roll
execute reboot
execute restore
execute scsi-dev
execute send-fds-statistics
execute set-next-reboot
execute sfp-mode-sgmii
execute shutdown
execute time
execute update-ase
execute update-av
execute update-ips
```

```
    execute update-now
    execute usb-disk
    execute vpn certificate ...
    get firewall vip ...
  end
```

History

FortiOS v3.0	New.
FortiOS v3.0 MR1	Added vdom-link, vpn, webfilter, execute backup, batch, dhcp lease-client, dhcp lease-list, fsae refresh, restore, telnet, and traceroute.
FortiOS v3.0 MR5	Added config firewall service, gui console, system console, system fortiguard, system replacemsg admin/alertemail/auth/nntp, vpn certificate crl/local/remote, execute central-mgmt, execute cfg ..., execute update-ips, and execute update-now.
FortiOS v3.0 MR6	Added `config system session-sync`, expanded command to `vpn certificate ...` . Removed `vpn sslvpn`.
FortiOS v4.0	Added `application, system replacemsg ec, system replacemsg nac-quar, system vdom-property, execute scsi-dev, execute sfpmode-sgmii, execute send-fsd-statistics, execute update-ase`.

Related topics

- vdom

vdom

From the super admin account, use this command to add and configure virtual domains. The number of virtual domains you can add is dependent on the FortiGate model. Virtual domain configuration (vdom-admin) must be enabled. See “system global” on page 423.

Once you add a virtual domain you can configure it by adding zones, firewall policies, routing settings, and VPN settings. You can also move physical interfaces from the root virtual domain to other virtual domains and move VLAN subinterfaces from one virtual domain to another.

By default all physical interfaces are in the root virtual domain. You cannot remove an interface from a virtual domain if the interface is part of any of the following configurations:

- routing
- proxy arp
- DHCP server
- zone
- firewall policy
- redundant pair
- link aggregate (802.3ad) group

Delete these objects, or modify them, to be able to remove the interface.

Note: You cannot delete the default root virtual domain, and you cannot delete a virtual domain that is used for system management.

Syntax

This command syntax shows how you access the commands within a VDOM. Refer to the relevant sections in this Reference for information on these commands.

```
config vdom
  edit <vdom_name>
    config antivirus
    config application
    config dlp
    config endpoint-control
    config firewall address, address6
    config firewall addrgrp, addrgrp6
    config firewall dnstranslation
    config interface-policy
    config interface-policy6
    config firewall ipmacbinding setting
    config firewall ipmacbinding table
    config firewall ippool
    config firewall ldb-monitor
    config firewall multicast-policy
    config firewall policy, policy6
    config firewall profile
    config firewall schedule onetime
    config firewall schedule recurring
    config firewall service custom
    config firewall service group
    config firewall shaper per-ip-shaper
    config firewall vip
```

```
config firewall vipgrp
config imp2p
config ips
config log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 |
   memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard}
   filter
config router
config spamfilter
config system admin
config system arp-table
config system dhcp reserved-address
config system dhcp server
config system gre-tunnel
config system interface
config system ipv6-tunnel
config system modem
config system proxy-arp
config system session-ttl
config system settings
config system sit-tunnel
config system wccp
config system zone
config user ban
config user ban
config user fsae
config user group
config user ldap
config user local
config user peer
config user peergrp
config user radius
config user setting
config user tacacs+
config vpn ...
config wanopt
config web-proxy
config webfilter
execute backup
execute clear system arp table
execute cli check-template-status
execute cli status-msg-only
execute dhcp lease-list
execute fsae refresh
execute ha disconnect
execute ha manage
execute ha synchronize
execute interface dhcpclient-renew
execute log delete-all
execute log delete-rolled
execute log display
execute log filter
execute log list
execute log roll
execute modem dial
```

```
    execute modem hangup
    execute modem trigger
    execute ping, ping6
    execute ping-options, ping6-options
    execute restore
    execute router clear bgp
    execute router clear ospf process
    execute router restart
    execute sfp-mode-sgmii
    execute ssh
    execute traceroute
    execute usb-disk
    execute vpn sslvpn del-tunnel
  next
  edit <another_vdom>
    config ...
    execute ...
  end
end
```

Variable	Description	Default
`edit <vdom_name>`	Enter a new name to create a new VDOM. Enter an existing VDOM name to configure that VDOM. The VDOM you enter becomes the current VDOM. A VDOM cannot have the same name as a VLAN. A VDOM name cannot exceed 11 characters in length.	

Note: The VDOM names `vsys_ha` and `vsys_fgfm` are in use by the FortiGate unit. If you attempt to name a new VDOM `vsys_ha` or `vsys_fgfm` it will generate an error.

Note: Use `config system settings set opmode {nat | transparent}` to set the operation mode for this VDOM to nat (NAT/Route) or transparent.

Example

This example shows how to add a virtual domain called Test1.

```
config system vdom
  edit Test1
end
```

History

FortiOS v3.0 New.

FortiOS v3.0 MR1 Added `system admin, interface, ipv6-tunnel` commands.
Added `batch, date, reboot, execute router clear ospf process` commands.
Removed `log fortianalyzer, log syslogd, log webtrends, router graceful-restart` commands.

FortiOS v3.0 MR1 Added `system setting multicast-forward and multicast-ttl-notchange`.

FortiOS v3.0 MR5 Removed config alertemail, and execute batch.
Added config gui, system arp-table, system proxy-arp, all of system settings.

FortiOS v3.0 MR7 Removed `config gui` and `system ipv6-tunnel`.
Added `system sit-tunnel`.

FortiOS v4.0 Added `config application, dlp, config endpoint-control, firewall interface-policy, firewall traffic-shape, system ipv6-tunnel, system modem, system wccp`. Added `execute interface, modem dial, modem hangup, ping6-options, sfp-mode-sgmii`, and `ssh`.

Related topics

- global

alertemail

Use `alertemail` commands to configure the FortiGate unit to monitor logs for log messages with certain severity levels. If the message appears in the logs, the FortiGate unit sends an email to a predefined recipient(s) of the log message encountered. Alert emails provide immediate notification of issues occurring on the FortiGate unit, such as system failures or network attacks.

Note: You must configure the server setting under `config system alertemail` before the commands under `config alertemail` become accessible. If vdoms are enabled, `config system alertemail` is a global command, and `config alertemail` is per VDOM. For more information, see "system alertemail" on page 392.

When configuring an alert email, you must configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server and must look up this name on your DNS server. See "dns" on page 413 for more information about configuring DNS servers.

This chapter contains the following section:

setting

Use this command to configure the FortiGate unit to send an alert email to up to three recipients. This command can also be configured to send an alert email a certain number of days before the FDS license expires and/or when the disk usage exceeds a certain threshold amount. You need to configure an SMTP server before configuring alert email settings. See “system alertemail” on page 392 for more information.

Note: The FortiGate unit must be able to look up the SMTP server name on your DNS server because the FortiGate unit uses the SMTP server to connect to the mail server. See “system dns” on page 413 for more information.

Syntax

```
config alertemail setting
  set username <user-name_str>
  set mailto1 <email-address_str>
  set mailto2 <email-address_str>
  set mailto3 <email-address_str>
  set filter-mode {category | threshold}
  set email-interval <minutes_int>
  set emergency-interval <minutes_int>
  set alert-interval <minutes_int>
  set critical-interval <minutes_int>
  set error-interval <minutes_int>
  set warning-interval <minutes_int>
  set notification-interval <minutes_int>
  set information-interval <minutes_int>
  set debug-interval <minutes_int>
  set severity {alert | critical | debug | emergency | error | information
     | notification | warning}
  set IPS-logs {disable | enable}
  set firewall-authentication-failure-logs {disable | enable}
  set HA-logs {enable | disable}
  set IPsec-error-logs {disable | enable}
  set FDS-update-logs {disable | enable}
  set PPP-errors-logs {disable | enable}
  set sslvpn-authentication-errors-logs {disable | enable}
  set antivirus-logs {disable | enable}
  set webfilter-logs {disable | enable}
  set configuration-changes-logs {disable | enable}
  set violation-traffic-logs {disable | enable}
  set admin-login-logs {disable | enable}
  set local-disk-usage-warning {disable | enable}
  set FDS-license-expiring-warning {disable | enable}
  set FDS-license-expiring-days <days_int>
  set local-disk-usage <percentage>
  set fortiguard-log-quota-warning {disable | enable}
end
```

Variable	Description	Default
username <user-name_str>	Enter a valid email address in the format user@domain.com. This address appears in the From header of the alert email.	No default.
mailto1 <email-address_str>	Enter an email address. This is one of the email addresses where the FortiGate unit sends an alert email.	No default.
mailto2 <email-address_str>	Enter an email address. This is one of the email addresses where the FortiGate unit sends an alert email.	No default.
mailto3 <email-address_str>	Enter an email address. This is one of the email addresses where the FortiGate unit sends an alert email.	No default.
filter-mode {category | threshold}	Select the filter mode of the alert email. The following fields display only when threshold is selected: • emergency-interval • alert-interval • critical-interval • error-interval • warning-interval • notification-interval • information-interval • debug-interval • severity	category
email-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out an alert email. This is not available when filter-mode is threshold.	5
emergency-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out alert email for emergency level messages. Only available when filter-mode is threshold.	1
alert-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out an alert email for alert level messages. Only available when filter-mode is threshold.	2
critical-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out an alert email for critical level messages. Only available when filter-mode is threshold.	3
error-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out an alert email for error level messages. Only available when filter-mode is threshold.	5
warning-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out an alert email for warning level messages. Only available when filter-mode is threshold.	10
notification-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out an alert email for notification level messages. Only available when filter-mode is threshold.	20
information-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out an alert email for information level messages. Only available when filter-mode is threshold.	30
debug-interval <minutes_int>	Enter the number of minutes the FortiGate unit should wait before sending out an alert email for debug level messages. Only available when filter-mode is threshold.	60

Variable	Description	Default
`severity {alert | critical | debug | emergency | error | information | notification | warning}`	Select the logging severity level. This is only available when `filter-mode` is `threshold`. The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select `error`, the unit logs `error`, `critical`, `alert`, and `emergency` level messages. `alert` – Immediate action is required. `critical` – Functionality is affected. `debug` – Information used for diagnosing or debugging the FortiGate unit. `emergency` – The system is unusable. `error` – An erroneous condition exists and functionality is probably affected. `information` – General information about system operations `notification` – Information about normal events. `warning` – Functionality might be affected.	`alert`
`IPS-logs {disable | enable}`	Enable or disable IPS logs.	`disable`
`firewall-authentication-failure-logs {disable | enable}`	Enable or disable firewall authentication failure logs.	`disable`
`HA-logs {enable | disable}`	Enable or disable high availability (HA) logs.	`disable`
`IPsec-error-logs {disable | enable}`	Enable or disable IPSec error logs	`disable`
`FDS-update-logs {disable | enable}`	Enable or disable FDS update logs.	`disable`
`PPP-errors-logs {disable | enable}`	Enable or disable PPP error logs.	`disable`
`sslvpn-authentication-errors-logs {disable | enable}`	Enable or disable SSL VPN authentication error logs.	`disable`
`antivirus-logs {disable | enable}`	Enable or disable antivirus logs.	`disable`
`webfilter-logs {disable | enable}`	Enable or disable web filter logs.	`disable`
`configuration-changes-logs {disable | enable}`	Enable or disable configuration changes logs.	`disable`
`violation-traffic-logs {disable | enable}`	Enable or disable traffic violation logs.	`disable`
`admin-login-logs {disable | enable}`	Enable or disable admin login logs	`disable`
`local-disk-usage-warning {disable | enable}`	Enable or disable local disk usage warning in percent. For example enter the number 15 for a warning when the local disk usage is at 15 percent. The number cannot be 0 or 100.	`disable`
`FDS-license-expiring-warning {disable | enable}`	Enable or disable to receive an email notification of the expire date of the FDS license.	`disable`
`FDS-license-expiring-days <days_int>`	Enter the number of days to be notified by email when the FDS license expires. For example, if you want notification five days in advance, enter 5.	`15`
`local-disk-usage <percentage>`	Enter a number for when the local disk's usage exceeds that number.	`75`
`fortiguard-log-quota-warning {disable | enable}`	Enable to receive an alert email when the FortiGuard Log & Analysis server reaches its quota.	`disable`

Examples

This example shows how to configure the user name, add three email addresses for sending alerts to, and what type of emails will contain which log messages, such as HA and antivirus.

```
config alertemail setting
  set username fortigate@ourcompany.com
  set mail1 admin1@ourcompany.com
  set mail2 admin2@ourcompany.com
  set mail3 admin3@ourcompany.com
  set filter-mode category
  set HA-logs enable
  set FDS-update-logs enable
  set antivirus-logs enable
  set webfilter-logs enable
  set admin-login-logs enable
  set violation-traffic-logs enable
end
```

History

FortiOS v2.80	Substantially revised and expanded.
FortiOS v3.0	Moved `authentication`, `server` and `password` to `config system alertemail`.
FortiOS v3.0MR2	New fields added for: • `IPS-logs` • `firewall-authentication-failure-logs` • `HA-logs` • `IPSec-errors-logs` • `FDS-update-logs` • `PPP-errors-logs` • `sslvpn-authentication-errors-logs` • `antivirus-logs` • `webfilter-logs` • `configuration-changes-logs` • `violation-traffic-logs` • `admin-login-logs` • `FDS-license-expiring-warning` • `local-disk-usage-warning` • `FDS-license-expiring-days` • `local-disk-usage`
FortiOS 3.0MR4	Added `fortiguard-log-quota-warning` field.

Related topics

- system alertemail
- system dns

antivirus

Use antivirus commands to configure antivirus scanning for services, quarantine options, and to enable or disable grayware and heuristic scanning.

This chapter contains the following sections:

filepattern

Use this command to add, edit or delete the file patterns used for virus blocking and to set which protocols to check for files to block.

If you need to add configuration via CLI that requires ? as part of config, you need to input CTRL-V first. If you enter the question mark (?) without first using CTRL-V, the question mark has a different meaning in CLI: it will show available command options in that section.

For example, if you enter ? without CTRL-V:

```
edit "*.xe
token line: Unmatched double quote.
```

If you enter ? with CTRL-V:

```
edit "*.xe?"
new entry '*.xe?' added
```

Syntax

```
config antivirus filepattern
  edit <filepattern_list_int>
    set name <filepattern_list_name>
    set comment <comment_str>
    config entries
      edit <filepattern_string>
        set action {allow | block}
        set active {ftp http im imap nntp pop3 smtp}
        set file-type {unknown | ignored | activemime | arj | aspack
            | base64 | bat | binhex | bzip | bzip2 | cab | jad | elf | exe
            | fsg | gzip | hlp | hta | html | javascript | lzh | msc
            | msoffice | mime | petite | prc | rar | class | sis | tar | upx
            | uue | cod | zip}
        set filter-type {pattern | type}
  end
```

Variable	Description	Default
<filepattern_list_int>	A unique number to identify the file pattern list.	
name <filepattern_list_name>	Enter a name for the file pattern header list.	
comment <comment_str>	Optionally enter a comment about to the file pattern header list.	
<filepattern_string>	The name of the file pattern being configured. This can be any character string.	
action {allow | block}	The action taken when a matching file is being transferred via a set active protocol. • Select allow to have the FortiGate unit allow matching files. • Select block to have the FortiGate unit block matching files. •	block
active {ftp http im imap nntp pop3 smtp}	The action specified will affect the file pattern in the selected protocols.	Varies.

Variable	Description	Default
`file-type {unknown | ignored | activemime | arj | aspack | base64 | bat | binhex | bzip | bzip2 | cab | jad | elf | exe | fsg | gzip | hlp | hta | html | javascript | lzh | msc | msoffice | mime | petite | prc | rar | class | sis | tar | upx | uue | cod | zip}`	This command is only available and valid when `filter-type` is set to `type`. Select the type of file the file filter will search for. Note that unlike the file pattern filter, this file type filter will examine the file contents to determine the what type of file it is. The file name and file extension is ignored. Because of the way the file type filter works, renaming files to make them appear to be of a different type will not allow them past the FortiGate unit without detection. Two of the available options are not file types: • Select `unknown` to configure a rule affecting every file format the file type filter unit does not recognize. Unknown includes every file format not available in the `file-type` command. • Select `ignored` to configure a rule affecting traffic the FortiGate unit typically does not scan. This includes primarily streaming audio and video.	`unknown`
`filter-type {pattern | type}`	Select the file filter detection method. • Enter `pattern` to examine files only by their names. For example, if `filter-type` is set to `pattern`, and the pattern is `*.zip`, all files ending in .zip will trigger this file filter. Even files ending in .zip that are not actually ZIP archives will trigger this filter. • Enter `type` to examine files only by their contents. Using the above example, if `filter-type` is set to `type`, and the type is `zip`, all ZIP archives will trigger this file filter. Even files renamed with non-zip file extensions will trigger this filter.	`pattern`

History

FortiOS v2.80 Substantially revised.

FortiOS v3.0 Added IM. Added multiple-list capability for models 800 and above.

FortiOS v4.0 Updated file-type options. The `file-type` option now available on all FortiGate models.

Related topics

- antivirus heuristic
- antivirus quarantine
- antivirus quarfilepattern
- antivirus service

heuristic

Use this command to configure heuristic scanning for viruses in binary files.

Syntax

```
config antivirus heuristic
  set mode {pass | block | disable}
end
```

Variable	Description	Default
mode {pass | block | disable}	Enter pass to enable heuristic scanning but pass detected files to the recipient. Suspicious files are quarantined if quarantine is enabled. Enter block to enable heuristic scanning and block detected files. A replacement message is forwarded to the recipient. Blocked files are quarantined if quarantine is enabled. Enter disable to disable heuristic scanning.	disable

Example

This example shows how to enable heuristic scanning.

```
config antivirus heuristic
  set mode pass
end
```

History

FortiOS v2.80 New.

FortiOS v3.0 MR7 The default value changes to “disable”.

Related topics

- antivirus filepattern
- antivirus quarantine
- antivirus quarfilepattern
- antivirus service

quarantine

Use this command to set file quarantine options.

FortiGate units with a local disk can quarantine blocked and infected files. The quarantined files are removed from the content stream and stored on the FortiGate local disk. Users receive a message informing them that the removed files have been quarantined.

FortiGate units that do not have a local disk can quarantine blocked and infected files to a FortiAnalyzer unit.

View the file names and status information about the file in the quarantined file list. Submit specific files and add file patterns to the autoupload list so they are automatically uploaded to Fortinet for analysis.

Syntax

```
config antivirus quarantine
  set agelimit <hours_int>
  set destination {disk | FortiAnalyzer | NULL}
  set drop-blocked {ftp http imap nntp pop3 smtp}
  set drop-heuristic {ftp http im imap nntp pop3 smtp}
  set drop-infected {ftp http im imap nntp pop3 smtp}
  set enable-auto-submit {disable | enable}
  set lowspace {drop-new | ovrw-old}
  set maxfilesize <MB_int>
  set sel-status {fileblocked heuristic}
  set store-blocked {ftp http imap nntp pop3 smtp}
  set store-heuristic {ftp http im imap nntp pop3 smtp}
  set store-infected {ftp http im imap nntp pop3 smtp}
  set use-fpat {enable | disable}
  set use-status {enable | disable}
end
```

Variable	Description	Default
`agelimit <hours_int>`	Specify how long files are kept in quarantine to a maximum of 479 hours. The age limit is used to formulate the value in the TTL column of the quarantined files list. When the limit is reached the TTL column displays EXP and the file is deleted (although a record is maintained in the quarantined files list). Entering an age limit of 0 (zero) means files are stored on disk indefinitely depending on low disk space action.	0
`destination {disk | FortiAnalyzer | NULL}`	The destination for quarantined files: • `disk` is the FortiGate unit internal hard disk, if present. • `FortiAnalyzer` is a FortiAnalyzer unit the FortiGate unit is configured to use. • `NULL` disables the quarantine. This command appears only if the FortiGate unit has an internal hard disk or is configured to use a FortiAnalyzer unit.	`NULL`
`drop-blocked {ftp http imap nntp pop3 smtp}`	Do not quarantine blocked files found in traffic for the specified protocols. The files are deleted.	`imap nntp`
`drop-heuristic {ftp http im imap nntp pop3 smtp}`	Do not quarantine files found by heuristic scanning in traffic for the specified protocols. NNTP support for this field will be added in the future.	`http im imap nntp pop3 smtp`

Variable	Description	Default
drop-infected {ftp http im imap nntp pop3 smtp}	Do not quarantine virus infected files found in traffic for the specified protocols. NNTP support for this field will be added in the future.	im imap nntp
enable-auto-submit {disable | enable}	Enable or disable automatic submission of the quarantined files matching the use-fpat or use-status settings.	disable
lowspace {drop-new | ovrw-old}	Select the method for handling additional files when the FortiGate hard disk is running out of space. Enter ovwr-old to drop the oldest file (lowest TTL), or drop-new to drop new quarantine files.	ovrw-old
maxfilesize <MB_int>	Specify, in MB, the maximum file size to quarantine. The FortiGate unit keeps any existing quarantined files over the limit. The FortiGate unit does not quarantine any new files larger than this value. The file size range is 0-499 MB. Enter 0 for unlimited file size.	0
sel-status {fileblocked heuristic}	Configure the status used for automatic uploading of quarantined files.	No default.
store-blocked {ftp http imap nntp pop3 smtp}	Quarantine blocked files found in traffic for the specified protocols. NNTP support for this field will be added in the future.	No default.
store-heuristic {ftp http im imap nntp pop3 smtp}	Quarantine files found by heuristic scanning in traffic for the specified protocols. NNTP support for this field will be added in the future.	No default.
store-infected {ftp http im imap nntp pop3 smtp}	Quarantine virus infected files found in traffic for the specified protocols. NNTP support for this field will be added in the future.	No default.
use-fpat {enable | disable}	Enable or disable using file patterns to select quarantined files for automatic uploading. See “antivirus quarfilepattern” on page 80 for information on how to configure the file patterns used for automatic uploading.	disable
use-status {enable | disable}	Enable or disable using file status to select quarantined files for automatic uploading.	disable

Example

This example shows how to set the quarantine age limit to 100 hours, not quarantine blocked files from SMTP and POP3 traffic, not quarantine heuristic tagged files from SMTP and POP3 traffic, enable auto submit to the quarantine, set the quarantine to drop new files if the memory is full, set the maximum file size to quarantine at 2 MB, quarantine files from IMAP traffic with blocked status, quarantine files with heuristic status in IMAP, HTTP, and FTP traffic., use both file patterns and status to determine which files to quarantine.

```
config antivirus quarantine
  set agelimit 100
  set drop-blocked smtp pop3
  set drop-heuristic smtp pop3
  set enable-auto-submit enable
  set lowspace drop-new
  set maxfilesize 2
  set sel-status fileblocked
  set store-blocked imap
  set store-heuristic imap http ftp
  set use-fpat enable
  set use-status enable
end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v2.80 MR2	The `enable_auto_upload` field was changed to `enable-auto-submit`.
FortiOS v3.0	Added IM and NNTP options.

Related topics

- antivirus filepattern
- antivirus heuristic
- antivirus quarfilepattern
- antivirus service

quarfilepattern

Use this command to configure the file patterns used by automatic file uploading. This command is only available on FortiGate units with a hard drive.

Configure the FortiGate unit to upload suspicious files automatically to Fortinet for analysis. Add file patterns to be uploaded to the autoupload list using the * wildcard character. File patterns are applied for autoupload regardless of file blocking settings.

Also upload files to Fortinet based on status (blocked or heuristics) or submit individual files directly from the quarantined files list. For more information, see antivirus quarantine.

Syntax

```
config antivirus quarfilepattern
  edit <pattern_str>
    set status {enable | disable}
  end
```

Variable	Description	Default
<pattern_str>	The file pattern to be quarantined.	
status {enable | disable}	Enable or disable using a file pattern.	disable

Example

Use the following commands to enable automatic upload of *.bat files.

```
config antivirus quarfilepattern
  edit *.bat
    set status enable
  end
```

History

FortiOS v2.80 New.

Related topics

- antivirus filepattern
- antivirus heuristic
- antivirus quarantine
- antivirus service

service

Use this command to configure how the FortiGate unit handles antivirus scanning of large files in HTTP, HTTPS, FTP, POP3, IMAP, and SMTP traffic and what ports the FortiGate unit scans for these services.

For HTTPS, you can only configure the ports.

Syntax

```
config antivirus service <service_str>
  set block-page-status-code <integer>
  set scan-bzip2 {enable | disable}
  set uncompnestlimit <depth_int>
  set uncompsizelimit <MB_int>
end
```

Variable	Description	Default
`<service_str>`	The service being configured: HTTP, HTTPS, FTP, IM, IMAP, NNTP, POP3, SMTP.	
`block-page-status-code <integer>`	Set a return code for HTTP replacement pages. This field is only for the HTTP service.	`200`
`scan-bzip2 {enable | disable}`	Enable to allow the antivirus engine to scan the contents of bzip2 compressed files. Requires antivirus engine 1.90 for full functionality. Bzip2 scanning is *extemely* CPU intensive. Unless this feature is required, leave `scan-bzip2` disabled.	`disable`
`uncompnestlimit <depth_int>`	Set the maximum number of archives in depth the AV engine will scan with nested archives. The limit is from 2 to 100. The supported compression formats are arj, bzip2, cab, gzip, lha, lzh, msc, rar, tar, and zip. Bzip2 support is disabled by default.	`12`
`uncompsizelimit <MB_int>`	Set the maximum uncompressed file size that can be buffered to memory for virus scanning. Enter a value in megabytes between 1 and the maximum oversize threshold. Enter “?” to display the range for your FortiGate unit. Enter 0 for no limit (not recommended).	`10` (MB)

Note: If the file in `uncompnestlimit` has more levels than the limit you set, or if the file in `uncompsizelimit` is larger than the limit you set, the file will pass through without being virus scanned.

How file size limits work

The uncompsizelimit applies to the uncompressed size of the file. If other files are included within the file, the uncompressed size of each one is checked against the uncompsizelimit value. If any one of the uncompressed files is larger than the limit, the file is passed without scanning, but the total size of all uncompressed files within the original file can be greater than the uncompsizelimit.

Example

This example shows how to set the maximum uncompressed file size that can be buffered to memory for scanning HTTP traffic at 15 MB.

```
config antivirus service http
  set uncompsizelimit 15
end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v2.80 MR6	Removed `diskfilesizelimit` field.
FortiOS v2.80 MR7	Added `uncompsizelimit` field.
FortiOS v3.0	Combined all services into one section. Added IM. Added `scan_bzip2`. Removed client comforting and file size limit commands.
FortiOS v3.0 MR3	Added support for HTTPS. But only ports can be configured.
FortiOS v3.0 MR7	Added return code selection for HTTP replacement pages.
FortiOS v4.0	Removed `port` field.

Related topics

- antivirus filepattern
- antivirus heuristic
- antivirus quarantine
- antivirus quarfilepattern

settings

Use this command to configure grayware detection as part of antivirus scanning.

Grayware programs are unsolicited commercial software programs that get installed on computers, often without the user's consent or knowledge. Grayware programs are generally considered an annoyance, but these programs can cause system performance problems or be used for malicious purposes.

Since grayware detection is part of antivirus scanning, antivirus scanning must be enabled for this setting to have any effect.

Syntax

```
config antivirus settings
  set grayware {enable | disable}
  end
```

Variable	Description	Default
`grayware {enable | disable}`	Enable or disable grayware detection.	`disable`

Example

Use the following commands to enable grayware detection.

```
config antivirus setttings
  set grayware enable
  end
```

History

FortiOS v4.00 New.

Related topics

- antivirus heuristic
- antivirus quarantine
- antivirus service

application

Use these commands to configure application control.

Application control is a UTM feature that allows your FortiGate unit to detect and take action against network traffic depending on the application generating the traffic. Based on FortiGate Intrusion Protection protocol decoders, application control is a more user-friendly and powerful way to use Intrusion Protection features to log and manage the behavior of application traffic passing through the FortiGate unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

The FortiGate unit can recognize the network traffic generated by more than 70 applications. You can create application control lists that specify what action will be taken with the traffic of the applications you need to manage. Specify the application control list in the protection profile applied to the network traffic you need to monitor. Create multiple application control lists, each tailored to a particular network, for example.

list

Use this command to create application control lists and configure the application options.

Syntax

```
config application list
  edit <app_list_str>
    config entries
      edit <id_integer>
        set action {block | pass}
        set application {<app_int> | All}
        set block-ack {enable | disable}
        set block-audio {enable | disable}
        set block-bye {enable | disable}
        set block-cancel {enable | disable}
        set block-encrypt {enable | disable}
        set block-file {enable | disable}
        set block-im {enable | disable}
        set block-info {enable | disable}
        set block-invite {enable | disable}
        set block-long-chat {enable | disable}
        set block-long-lines {enable | disable}
        set block-mcast {enable | disable}
        set block-message {enable | disable}
        set block-notify {enable | disable}
        set block-options {enable | disable}
        set block-photo {enable | disable}
        set block-prack {enable | disable}
        set block-publish {enable | disable}
        set block-refer {enable | disable}
        set block-register {enable | disable}
        set block-subscribe {enable | disable}
        set block-unknown {enable | disable}
        set block-update {enable | disable}
        set call-keepalive <minutes_int>
        set category {<cat_int> | All}
        set comment <comment_string>
        set im-no-content-summary {enable | disable}
        set imoversizechat <bytes_int>
        set inspect-anyport {enable | disable}
        set invite-rate <rate_int>
        set log {disable | enable}
        set max-calls <calls_int>
        set max-dialogs <calls_int>
        set max-line-length <length_int>
        set message-rate <rate_int>
        set open-contact-pinhole {disable | enable}
        set open-register-pinhole {disable | enable}
        set other-application-action {block | pass}
        set other-application-log {enable | disable}
        set reg-diff-port {enable | disable}
        set register-rate <rate_int>
        set rfc2543-branch {enable | disable}
```

```
        set rtp {enable | disable}
        set sccp-log-violations {enable | disable}
        set sccp-no-content-summary {enable | disable}
        set session-ttl <ttl_int>
        set shaper <profile_str>
        set shaper-reverse <profile
        set sip-log-violations {enable | disable}
        set strict-register {enable | disable}
        set verify-header {enable | disable}
      end
    end
    set comment <comment_string>
    set other-application-action {block | pass}
    set other-application-log {enable | disable}
end
```

Variable	Description	Default
<app_list_str>	The name of the application control list.	No default.
<id_integer>	Enter the unique ID of the list entry you want to edit, or enter an unused ID to create a new one.	
action {block | pass}	Enter the action the FortiGate unit will take with traffic from the application of the specified type. • block will stop traffic from the specified application. • pass will allow traffic from the specified application.	block
application {<app_int> | All}	Enter the application integer to specify an individual application, or enter All to include all applications in the currently specified category. Enter set application ? to list all application integers in the currently configured category.	all
block-ack {enable | disable}	Enable to block SIP ACK requests. This command is available only when application is set to SIP.	disable
block-audio {enable | disable}	Enable to block audio. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.	disable
block-bye {enable | disable}	Enable to block SIP BYE requests. This command is available only when application is set to SIP.	disable
block-cancel {enable | disable}	Enable to block SIP CANCEL requests. This command is available only when application is set to SIP.	disable
block-encrypt {enable | disable}	Enable to block encrypted IM sessions. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.	disable
block-file {enable | disable}	Enable to block IM file transfers. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.	disable
block-im {enable | disable}	Enable to block instant messages. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.	disable
block-info {enable | disable}	Enable to block SIP INFO requests. This command is available only when application is set to SIP.	disable

Variable	Description	Default
block-invite {enable | disable}	Enable to block SIP INVITE requests. This command is available only when application is set to SIP.	disable
block-long-chat {enable | disable}	Enable to block oversized chat messages. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.	disable
block-long-lines {enable | disable}	Enable to block SIP requests with headers exceeding the value set in max-line-length. This command is available only when application is set to SIP.	enable
block-mcast {enable | disable}	Enable to block multicast RTP connections. This command is available only when application is set to SCCP.	disable
block-message {enable | disable}	Enable to block SIMPLE instant messages. This command is available only when application is set to SIMPLE.	disable
block-notify {enable | disable}	Enable to block SIP NOTIFY requests. This command appears only when application is set to SIP.	disable
block-options {enable | disable}	Enable to block SIP OPTIONS requests. This command is available only when application is set to SIP.	disable
block-photo {enable | disable}	Enable to block IM photo sharing. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.	disable
block-prack {enable | disable}	Enable to block SIP PRACK requests. This command is available only when application is set to SIP.	disable
block-publish {enable | disable}	Enable to block SIP PUBLISH requests. This command is available only when application is set to SIP.	disable
block-refer {enable | disable}	Enable to block SIP REFER requests. This command is available only when application is set to SIP.	disable
block-register {enable | disable}	Enable to block SIP REGISTER requests. This command is available only when application is set to SIP.	disable
block-subscribe {enable | disable}	Enable to block SIP SUBSCRIBE requests. This command is available only when application is set to SIP.	disable
block-unknown {enable | disable}	Enable to block unrecognized SIP requests. This command is available only when application is set to SIP.	enable
block-update {enable | disable}	Enable to block SIP UPDATE requests. This command is available only when application is set to SIP.	disable
call-keepalive <minutes_int>	Enter the number of minutes the FortiGate unit will continue tracking SIP calls with no RTP. This command is available only when application is set to SIP.	0

Variable	Description	Default
category {<cat_int> | All}	Enter the category integer to specify an application category, or enter All to include all categories. Set a specific category to limit the scope of the All setting of the application command. For example, setting category to im and application to All will have the list entry include all IM applications. Similarly, the applications listed with the set application ? command will be limited to the currently configured category. Enter set category ? to list all category integers.	All
comment <comment_string>	Optionally, enter a descriptive comment.	No default.
im-no-content-summary {enable | disable}	Enable to prevent display of content information on the dashboard. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.	disable
imoversizechat <bytes_int>	Enter the maximum length of chat messages, in bytes. The value must be between 2048 and 65536. This command appears only when application is set to AIM.	8192
inspect-anyport {enable | disable}	Enable to inspect all ports not used by any proxy for IM traffic. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.	disable
invite-rate <rate_int>	Enter the maximum number of SIP INVITE requests per second, per policy. This command appears only when application is set to SIP.	0
log {disable | enable}	Enable to have the FortiGate until log the occurrence and the action taken if traffic from the specified application is detected.	enable
max-calls <calls_int>	Enter the maximum number of calls calls per minute per SCCP client. The value can not exceed 65535. This command is available only when application is set to SCCP.	0
max-dialogs <calls_int>	Enter the maximum number of concurrent SIP dialogs. This command appears only when application is set to SIP.	0
max-line-length <length_int>	Enter the maximum SIP header line length. The value must be between 78 and 4096. Enable block-long-lines to enforce this limit. This command is available only when application is set to SIP.	998
message-rate <rate_int>	Enter the maximum number of MESSAGE requests per second, per policy. This command is available only when application is set to SIMPLE.	0
open-contact-pinhole {disable | enable}	Open or close SIP pinholes for non-REGISTER SIP requests (usually INVITE requests). By default open-contact-pinhole is enabled and the FortiGate unit opens pinholes for non-REGISTER requests. Set to disable to prevent the FortiGate unit from opening these pinholes. This command is available only when application is set to SIP.	enable
open-register-pinhole {disable | enable}	Open or close SIP pinholes for SIP REGISTER requests. By default open-register-pinhole is enabled and the FortiGate unit opens pinholes for REGISTER requests. Set to disable prevent the FortiGate unit from opening these pinholes. This command is available only when application is set to SIP.	enable
other-application-action {block | pass}	Enter the action the FortiGate unit will take for unrecognized application traffic or supported application traffic not configured in the current application control list.	pass

Variable	Description	Default
other-application-log {enable | disable}	Enter the logging action the FortiGate unit will take for unrecognized application traffic or supported application traffic not configured in the current application control list.	disable
reg-diff-port {enable | disable}	Enable to accept SIP REGISTER responses even if the source port is different from the destination port in the register request. This command is available only when application is set to SIP.	disable
register-rate <rate_int>	Enter the maximum number of SIP REGISTER requests per second, per policy. This command is available only when application is set to SIP.	0
rfc2543-branch {enable | disable}	Enable to support RFC 2543-complaint SIP calls involving branch commands that are missing or that are valid for RFC 2543 but are invalid for RFC 3261. RFC 3261 is the most recent SIP RFC. RFC 3261 obsoletes RFC 2543. This command is available only when application is set to SIP.	disable
rtp {enable | disable}	Enable to allow RTP traffic. This command is available only when application is set to SIP.	enable
sccp-log-violations {enable | disable}	Enable to log SCCP violations. This command is available only when application is set to SCCP.	disable
sccp-no-content-summary {enable | disable}	Enable to prevent display of content information on the dashboard. This command is available only when application is set to SCCP.	disable
session-ttl <ttl_int>	Enter the application's session TTL. Enter 0 to disable this option. If this option is not enabled, the TTL defaults to the setting of the config system session-ttl CLI command.	0
shaper <profile_str>	Enter the name of a traffic shaping profile to enable traffic shaping. Traffic flowing from the source to the destination as specified in the firewall policy is subject to the specified traffic shaping policy. This option is available for some P2P applications. For information about traffic shaping profiles, see "firewall shaper traffic-shaper" on page 180.	No default
shaper-reverse <profile	Enter the name of a traffic shaping profile to enable traffic shaping. Traffic flowing from the destination to the source as specified in the firewall policy is subject to the specified traffic shaping policy. This option is available for some P2P applications. For information about traffic shaping profiles, see "firewall shaper traffic-shaper" on page 180.	No default
sip-log-violations {enable | disable}	Enable to log SIP violations. This command is available only when application is set to SIP.	disable
strict-register {enable | disable}	Enable to allow only the registrar to connect. This command is available only when application is set to SIP.	disable
verify-header {enable | disable}	Enable to verify SCCP header content. This command is available only when application is set to SCCP.	disable

History

FortiOS v4.0	New.
FortiOS 4.0 MR1	Added fields `open-contact-pinhole`, `open-register-pinhole`, and `rfc2543-branch` SIP-related fields. Removed the `sccp-archive-full`, `sccp-archive-summary`, `simple-archive-full`, `simple-archive-summary`, `sip-archive-summary`, and `sip-archive-full` fields.

Related commands

- application name

name

Use this command to view the settings of each application. The application category and ID are displayed. This command is ‘read only’ and cannot be used to change application settings.

Syntax

```
config application name <app_str>
  get
end
```

Variable	Description	Default
`name <app_str>`	Enter the name of the application you want to view. Enter `config application name ?` to list all the applications.	No default

History

FortiOS v4.0 New.

Related commands

- application list

dlp

The FortiGate data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. You can define sensitive data patterns, and data matching these patterns will be blocked and/or logged when passing through the FortiGate unit. The DLP system is configured by creating individual rules, combining the rules into DLP sensors, and then assigning a sensor to a protection profile.

For more information about DLP see the *FortiGate UTM User Guide*.

Use these commands to configure Data Leak Prevention (DLP).

compound

Use this command to add or edit DLP compound rules. DLP compound rules are groupings of DLP rules that also change the way they behave when added to a DLP sensor. Individual rules can be configured with only a single attribute. When this attribute is discovered in network traffic, the rule is activated.

Compound rules allow you to group individual rules to specify far more detailed activation conditions. Each included rule is configured with a single attribute, but every attribute must be present before the rule is activated.

For example, create two rules and add them to a sensor:

- Rule 1 checks SMTP traffic for a sender address of spammer@example.com
- Rule 2 checks SMTP traffic for the word “sale” in the message body

When the sensor is used, either rule could be activated if its configured condition is true. If only one condition is true, only the corresponding rule would be activated. Depending on the contents of the SMTP traffic, neither, either, or both could be activated.

If you remove these rules from the sensor, add them to a compound rule, and add the compound rule to the sensor, the conditions in both rules have to be present in network traffic to activate the compound rule. If only one condition is present, the message passes without any rule or compound rule being activated.

By combining the individually configurable attributes of multiple rules, compound rules allow you to specify far more detailed and specific conditions to trigger an action.

Syntax

```
config dlp compound
  edit <compound_rule_str>
    set comment <comment_str>
    set member <rule1> [<rule2> ...]
    set protocol {email | ftp | http | im | nntp}
    set sub-protocol <sub_protocol_1> [<sub_protocol_2> ...]
  end
```

Variable	Description	Default
`compound_rule_str`	The name of the compound rule.	No default.
`comment <comment_str>`	Optionally, enter a descriptive comment. Enclose the comment in quotes if you want to include spaces.	No default.
`member <rule1> [<rule2> ...]`	Enter a space-delimited list of DLP rules that belong to this compound rule. For information about creating rules, see “dlp rule” on page 96.	No default.
`protocol {email | ftp | http | im | nntp}`	Select the protocol to which this compound rule applies.	No default.
`sub-protocol <sub_protocol_1> [<sub_protocol_2> ...]`	Select the sub-protocols to which this compound rule applies. This is not available if `protocol` is `nntp`. For other protocols, the available sub-protocols are: • http: `http-get`, `http-post` • email: `smtp`, `pop3`, `imap` • ftp: `ftp-get`, `ftp-put` • im: `aim` (AOL IM), `icq`, `msn`, `ym` (Yahoo IM) If your FortiGate unit supports SSL content scanning and inspection, the following sub-protocols are also available: • http: `https-get`, `https-post` • email: `smtps`, `pop3s`, `imaps` Separate multiple sub-protocol names with a space.	No default.

Example

Use the following command to add a compound rule called pop3_comp that includes three rules named pop3_rule_1, pop3_rule_2, and pop3_rule_3.

```
config dlp compound
  edit pop3_comp
    set protocol email
    set sub-protocol pop3
    set member pop3_rule_1 pop3_rule_2 pop3_rule_3
    set comment "Compound rule for POP3"
  end
```

History

FortiOS v4.0 New.

Related commands

- dlp rule
- dlp sensor

rule

Use this command to add or edit DLP rules. DLP rules are the core element of the data leak prevention feature. These rules define the data to be protected so the FortiGate unit can recognize it. For example, an included rule uses regular expressions to describe Social Security number:

```
([0-6]\d{2}|7([0-6]\d|7[0-2]))[ \-]?\d{2}[ \-]\d{4}
```

Rather than having to list every possible Social Security number, this regular expression describes the structure of a Social Security number. The pattern is easily recognizable by the FortiGate unit.

DLP rules can be combined into compound rules and they can be included in sensors. If rules are specified directly in a sensor, traffic matching any single rule will trigger the configured action. If the rules are first combined into a compound rule and then specified in a sensor, every rule in the compound rule must match the traffic to trigger the configured action.

Individual rules in a sensor are linked with an implicit OR condition while rules within a compound rule are linked with an implicit AND condition.

Syntax

```
config dlp rule
  edit rule_name <rule_str>
    set description <desc_str>
    set field {always | attachment-size | attachment-text | attachment-type
       | body | cgi-parameters | cookie-content | encrypted | file-pattern
       | file-text | file-type | header | hostname | receiver | sender
       | server | subject | transfer-size | url | user | user-group}
    set file-pattern <pattern_str>
    set file-pattern-negated {enable | disable}
    set file-scan {archive-content archive-whole ms-word-content
       ms-word-whole pdf-content pdf-whole}
    set file-type <type_int>
    set file-type-negated {enable | disable}
    set negated {enable | disable}
    set operator {equal | greater-equal | less-equal | not-equal}
    set protocol {email | http | ftp | nntp | im | session-ctrl}
    set regexp <regex_str>
    set regexp-negated {enable | disable}
    set regexp-wildcard {enable | disable}
    set regexp-utf8 {enable | disable}
    set rule_name <rule_str>
    set string <str>
    set string-negated {enable | disable}
    set sub-protocol <sub_protocol_1> [<sub_protocol_2> ...]
    set value <value_int>
  end
```

Variable	Description	Default
`description <desc_str>`	Enter an optional description of the DLP rule. Enclose the description in quotes if you want to include spaces.	No default
`field {always | attachment-size | attachment-text | attachment-type | body | cgi-parameters | cookie-content | encrypted | file-pattern | file-text | file-type | header | hostname | receiver | sender | server | subject | transfer-size | url | user | user-group}`	Enter the attribute the DLP rule will examine for a match. The available fields will depend on the protocol and sub-protocol you've set. `always` — Match all transfers. This option is available for all protocols. `attachment-size` — Check the attachment file size. This option is available for Email. `attachment-text` — Check the attachment for a text string. This option is available for Email. `attachment-type` — Search email messages for file types or file patterns as specified in the selected file filter. This option is available for Email. `body` — Search for text in the message or page body. This option is available for Email, HTTP, and NNTP. `cgi-parameters` — Search for a CGI parameter in any web page with CGI code. This option is available for HTTP. `cookie-content` — Search the contents of cookies for a text string. This option is available for HTTP. `encrypted` — Check whether files are or are not encrypted. Encrypted files are archives and MS Word files protected with passwords. Because they are password protected, the FortiGate unit cannot scan the contents of encrypted files. `file-pattern` — Search for file patterns and file types. The patterns and types configured in file filter lists and a list is selected in the DLP rule. This option is available for FTP, HTTP, IM, and NNTP. `file-text` — Search for text in transferred text files. This option is available in FTP, IM, and NNTP. `file-type` — Search for file patterns and file types. The patterns and types configured in file filter lists and a list is selected in the DLP rule. This option is available for FTP, HTTP, IM, and NNTP. `header` — Search for a text string in HTTP headers. `hostname` — Search for the host name when contacting a HTTP server. `receiver` — Search for a text string in the message recipient email address. This option is available for Email. `sender` — Search for a text string in the message sender user ID or email address. This option is available for Email and IM. `server` — Search for the server's IP address in a specified address range. This option is available for FTP, NNTP. `subject` — Search for a text string in the message subject. This option is available for Email. `transfer-size` — Check the total size of the information transfer. In the case of email traffic for example, the transfer size includes the message header, body, and any encoded attachment. `url` — Search for the specified URL in HTTP traffic. `user` — Search for traffic from an authenticated user. `user-group` — Search for traffic from any authenticated user in a user group.	`body`
`file-pattern <pattern_str>`	Enter a base-64 string the FortiGate unit will search for in files. A match will trigger the rule.	No default
`file-pattern-negated {enable | disable}`	Enable to trigger the rule when a file does not contain the pattern specified with the `file-pattern` command.	`disable`

Variable	Description	Default
file-scan {archive-content archive-whole ms-word-content ms-word-whole pdf-content pdf-whole}	You can select file options for any protocol to configure how the DLP rule handles archive files, MS-Word files, and PDF files found in content traffic. Note: Office 2007/2008 DOCX files are not recognized as MS-Word by the DLP scanner. To scan the contents of DOCX files, select the archive-content option. archive-content — When selected, files within archives are extracted and scanned in the same way as files that are not archived. archive-whole — When selected, archives are scanned as a whole. The files within the archive are not extracted and scanned individually. ms-word-content — When selected the text contents of MS Word DOC documents are extracted and scanned for a match. All metadata and binary information is ignored. ms-word-whole — When selected, MS Word DOC files are scanned. All binary and metadata information is included. If you are scanning for text entered in a DOC file, use the Scan MS-Word option. Binary formatting codes and file information may appear within the text, causing text matches to fail. pdf-content — When selected, the text contents of PDF documents are extracted and scanned for a match. All metadata and binary information is ignored. pdf-whole — When selected, PDF files are scanned. All binary and metadata information is included. If you are scanning for text in PDF files, use the Scan PDF Text option. Binary formatting codes and file information may appear within the text, causing text matches to fail.	null
file-type <type_int>	When you set the field command to file-type, use the file-type command to specify which file-type list is used. The <type_int> variable corresponds to the list position in the *UTM* > *AntiVirus* > *File Filter* list in the web-based manager. For example, enter 3 to specify the third list.	No default
file-type-negated {enable | disable}	Enable to trigger the rule when the file type does not match that specified with the file-type command.	disable
negated {enable | disable}	When the field command is set to encrypted, password protected archives and MS Word documents trigger the rule. To reverse this behavior and trigger the rule when archives and MS Word documents are not password protected, set negated to enable.	disable
operator {equal | greater-equal | less-equal | not-equal}	When the FortiGate unit checks sizes or quantities, an operator must be used to specify when the rule is triggered. The operators are: equal — The rule is triggered when the stated quantity is equal to the quantity detected. greater-equal — The rule is triggered when the stated quantity is greater then or equal to the quantity detected. less-equal — The rule is triggered when the stated quantity is less than or equal to the quantity detected. not-equal — The rule is triggered when the stated quantity is not equal to the quantity detected. The detected quantity can be greater than or less than the stated quantity.	equal
protocol {email | http | ftp | nntp | im | session-ctrl}	Select the type of content traffic to which the DLP rule the rule will apply. The available rule options vary depending on the protocol that you select.	No default
regexp <regex_str>	Enter the regular expression or wildcard to test. Use the regexp-wildcard field to choose between regular expression syntax and wildcards.	No default
regexp-negated {enable | disable}	By default, DLP rules are triggered when the FortiGate unit discovers network traffic that matches the regular expressions or wildcards specified in DLP rules. Enable regexp-negated to have the DLP rule triggered when traffic ***does not*** match the regular expression or wildcard specified in the rule.	disable

Variable	Description	Default
`regexp-wildcard {enable | disable}`	DLP rule expressions can be written using regular expressions or wildcards. Enable `regexp-wildcard` to use wildcards and disable it to use regular expressions.	`disable`
`regexp-utf8 {enable | disable}`	Either ASCII or UTF-8 encoding can be used when comparing rules with network traffic. Enable `regexp-utf8` to use UTF-8 encoding and disable it to use plain ASCII.	`disable`
`rule_name <rule_str>`	Enter the name of the rule you want to edit. Enter a new name to create a DLP rule.	No default
`string <str>`	When the field command is set to `user` or `user-group`, use the string command to specify the user name or user-group name.	No default
`string-negated {enable | disable}`	Enable `string-negated` to have the DLP rule triggered when the user or user-group specified with the `string` command ***does not*** match.	`disable`
`sub-protocol <sub_protocol_1> [<sub_protocol_2> ...]`	Set the sub-protocols to which this rule applies. This is not available if `protocol` is `nntp`. For other protocols, the available sub-protocols are: • http: `http-get`, `http-post` • email: `smtp`, `pop3`, `imap` • ftp: `ftp-get`, `ftp-put` • im: `aim` (AOL IM), `icq`, `msn`, `ym` (Yahoo IM) • session-ctrl: `sip`, `simple`, `sccp` If your FortiGate unit supports SSL content scanning and inspection, the following sub-protocols are also available: • http: `https-get`, `https-post` • email: `smtps`, `pop3s`, `imaps` Separate multiple sub-protocol names with a space.	`null`
`value <value_int>`	Field types that search for matches based on numbers require a number be specified with the `value` command. For example, the `attachment-size` command checks attachments based on their size, measured in kilobytes.	`0`

Example

Use the following command to add a rule called `pop3_rule_1` for the email protocol and the POP3 sub-protocol that scans the send field of all POP3 email messages for the email address: user@example.com.

```
config dlp rule
  edit pop3_rule_1
    set protocol email
    set sub-protocol pop3
    set field sender
    set set regexp user@exmple.com
    set description “Search POP3 for user@example.com”
  end
```

History

FortiOS v4.0 New.

FortiOS 4.0 MR1 `always` option for the `field` field added. `session-ctrl` option of the `protocol` field added.

Related commands

- dlp compound
- dlp sensor

sensor

Use this command to create a DLP sensor. DLP sensors are simply collections of DLP rules and DLP compound rules. The DLP sensor also includes settings such as action, archive, and severity for each rule or compound rule. Once a DLP sensor is configured, it can be specified in a protection profile. Any traffic handled by the policy in which the protection profile is specified will enforce the DLP sensor configuration.

Syntax

```
config dlp sensor
  edit <sensor_str>
    set comment <comment_str>
    config rule
      edit <rule_str>
        set action {ban | ban-sender | block | exempt | log-only
            | quarantine-ip | quarantine-port}
        set archive {disable | enable | summary-only}
        set expiry {<int>d | <int>h | <int>m | indefinite}
        set severity <severity_int>
        set status {enable | disable}
      next
    config compound-rule
      edit <compound-rule_str>
        set action {ban | ban-sender | block | exempt | log-only
            | quarantine-ip | quarantine-port}
        set archive {disable | enable | summary-only}
        set expiry {<int>d | <int>h | <int>m | indefinite}
        set severity <severity_int>
        set status {enable | disable}
      next
    end
  end
```

Variable	Description	Default
<sensor_str>	Enter the name of a sensor to edit. Enter a new name to create a new DLP sensor.	No default
comment <comment_str>	Enter an optional description of the DLP sensor. Enclose the description in quotes if you want to include spaces.	No default
edit <rule_str>	Add a rule to a sensor by specifying the name of a DLP rule that has already been added.	
edit <compound-rule_str>	Add a compound rule to a sensor by specifying the name of a DLP compound rule that has already been added.	

Variable	Description	Default
`action {ban | ban-sender | block | exempt | log-only | quarantine-ip | quarantine-port}`	Enter the action taken when the rule is triggered. `ban` — Block all traffic to or from the user using the protocol that triggered the rule and add the user to the Banned User list if the user is authenticated. If the user is not authenticated, block all traffic of the protocol that triggered the rule from the user's IP address. `ban-sender` — Block email or IM traffic from the sender of matching email or IM messages and add the sender to the Banned User list. This action is available only for email and IM protocols. For email, the sender is determined by the From: address in the email header. For IM, all members of an IM session are senders and the senders are determined by finding the IM user IDs in the session. `block` prevents the traffic matching the rule from being delivered. `exempt` — Prevent any DLP sensors from taking action on matching traffic. This action overrides any other action from any matching sensors. `log-only` — Prevent the DLP rule from taking any action on network traffic but log the rule match. Other matching rules in the same sensor and other sensors may still operate on matching traffic. `quarantine-ip` — Block access through the FortiGate unit for any IP address that sends traffic matching a sensor with this action. The IP address is added to the Banned User list. `quarantine-port` — Block access to the network from any client on the interface that sends traffic matching a sensor with this action.	`log-only`
`archive {disable | enable | summary-only}`	Configure DLP archiving for the rule or compound rule. `disable` — disable DLP archiving for the rule or compound rule. This option is not valid if the rule or compound rule protocol is `session-ctrl`. `enable` — enable full DLP archiving for the rule or compound rule. `summary-only` — enable summary DLP archiving for the rule or compound rule. DLP archiving requires a FortiAnalyzer unit or the FortiGuard Analysis and Management Service.	`disable`
`expiry {<int>d | <int>h | <int>m | indefinite}`	For the actions `ban`, `ban-sender`, `quarantine-ip`, and `quarantine-port`, you can set the duration of the ban/quarantine. The duration can be indefinite or a specified number of days, hours, or minutes. `<int>d` — Enter the number of days followed immediate with the letter 'd'. For example, `7d` represents seven days. `<int>h` — Enter the number of hours followed immediate with the letter 'h'. For example, `12h` represents 12 hours. `<int>m` — Enter the number of minutes followed immediate with the letter 'm'. For example, `30m` represents 30 minutes. `indefinite` — Enter `indefinite` to keep the ban/quarantine active until the user or IP address is manually removed from the banned user list.	`indefinite`

Variable	Description	Default
severity <severity_int>	Enter the severity of the content that the rule or compound rule is a match for. <severity_int> is an integer from 1 to 5. Use the severity to indicate the seriousness of the problems that would result from the content passing through the FortiGate unit. For example, if the DLP rule finds high-security content the severity could be 5. On the other hand if the DLP rule finds any content the severity should be 1. DLP adds the severity to the severity field of the log message generated when the rule or compound rule matches content. The higher the number the greater the severity.	1
status {enable | disable}	You can disable a sensor rule or compound rule by setting status to disable. The item will be listed as part of the sensor, but it will not be used.	disable

Example

Use the following command to add a DLP sensor named New_sensor and add two rules and two compound rules to the sensor.

```
config dlp sensor
  set comment "A useful DLP Sensor"
  config rule
    edit All_Email
      set action log-only
      set archive summary-only
    next
    edit FTP-action
      set action block
      set severity 3
      set archive enable
    end
  config compound-rule
    edit Email-SIN
      set action log-only
      set archive summary-only
    next
    edit Email-action
      set action block
      set severity 4
      set archive disable
    end
  end
```

History

FortiOS v4.0	New.
FortiOS 4.0 MR1	summary-only option for the archive field added. severity field added.

Related commands

- dlp compound
- dlp rule

endpoint-control

Use endpoint-control commands to configure the following parts of the Endpoint NAC feature:

- application detection rules
- Endpoint NAC profiles
- the required minimum version of FortiClient Endpoint Security
- the FortiClient installer download location

Endpoint NAC is enabled in firewall policies.

This chapter contains the following sections:

apps-detect rule-list

Use this command to configure the application detection part of the Endpoint NAC feature. Endpoint NAC must be enabled in the firewall policy.

Syntax

```
config endpoint-control apps-detect rule-list
  edit <rule_list_name>
    set comment <comment_str>
    set other-application-action {allow | deny | monitor}
    config entries
      edit <rule_id>
        set category <category_id>
        set vendor <vendor_id>
        set application <application_id>
        set action {allow | deny | monitor}
        set status {installed | running}
      end
  end
```

Variable	Description	Default
<app-name>	Enter a descriptive name for the application.	No default.
<rule_list_name>	Enter the application rule list name.	
action {allow | deny | monitor}	Select what to do if this application is running on the endpoint: • allow — allow the endpoint to connect • deny — block the endpoint • monitor — include endpoint's information in statistics and logs	deny
application <application_id>	Select the application ID. Enter 0 for all applications. For a list of applications, enter set application ?	0
category <category_id>	Enter the application category ID. Enter 0 for all categories. For a list of category IDs, enter set category ?	0
comment <comment_str>	Optionally enter a descriptive comment.	No default.
other-application-action {allow | deny | monitor}	Select what to do if applications not included in this list are running on the endpoint: • allow — allow the endpoint to connect • deny — block the endpoint • monitor — include endpoint's information in statistics and logs	monitor
status {installed | running}	Select running to take action only if the application is running.	installed
vendor <vendor_id>	Enter the vendor ID. Enter 0 for all vendors. For a list of vendor IDs, enter set vendor ?	0

History

FortiOS v4.0 New.

FortiOS v4.0 MR1 New command replaces endpoint-control apps-detection.

Related commands

- endpoint-control settings
- firewall policy, policy6

profile

Use this command to configure an Endpoint NAC profile.

Syntax

```
config endpoint-control profile
  edit <profile_name>
    set application-detection {enable | disable}
    set application-detection-rule-list <rulelist_name>
    set feature-enforcement {enable | disable}
    set recommendation-disclaimer {enable | disable}
    set require-av {enable | disable}
    set require-avuptodate {enable | disable}
    set require-firewall {enable | disable}
    set require-license {enable | disable}
    set require-webfilter {enable | disable}
  end
```

Variable	Description	Default
<profile_name>	Enter a name for this Endpoint NAC profile.	No default.
application-detection {enable | disable}	Enable application detection.	disable
application-detection-rule-list <rulelist_name>	Enter the name of the application rule list to use. See "endpoint-control apps-detect rule-list" on page 104. This is available if application-detection is enabled.	No default.
feature-enforcement {enable | disable}	Enable to deny access to endpoints that do not have FortiClient Endpoint Security installed.	disable
recommendation-disclaimer {enable | disable}	Enable to use Endpoint NAC Recommendation Portal replacement message, which allows user to continue without installing FortiClient Endpoint Security. Disable to use Endpoint NAC Download Portal replacement message, which only allows user to download FortiClient Endpoint Security installer.	enable
require-av {enable | disable}	Enable to deny access to endpoints that do not have the FortiClient antivirus feature enabled. This is available if feature-enforcement is enabled.	disable
require-avuptodate {enable | disable}	Enable to deny access to endpoints with out-of-date FortiClient antivirus signatures. This is available if feature-enforcement and require-av are enabled.	disable
require-firewall {enable | disable}	Enable to deny access to endpoints that do not have the FortiClient firewall enabled. This is available if feature-enforcement is enabled.	disable
require-license {enable | disable}	Enable to deny access to endpoints on which FortiClient is not licensed. This is available if feature-enforcement is enabled.	disable
require-webfilter {enable | disable}	Enable to deny access to endpoints that do not have the FortiClient web filter feature enabled. This is available if feature-enforcement is enabled.	disable

History

FortiOS v4.0 MR1 New.

Related commands

- endpoint-control apps-detect rule-list
- endpoint-control settings
- firewall policy, policy6

settings

Use this command to configure the required minimum version of FortiClient Endpoint Security and the installer download location. This is part of the Endpoint Control feature.

Syntax

```
config endpoint-control settings
  set compliance-timeout <minutes>
  set download-location {custom | fortigate | fortiguard}
  set download-custom-link <url>
  set enforce-minimum-version {enable | disable}
  set version <major.minor.patch>
  set version-check {latest | minimum}
  end
```

Variable	Description	Default
`compliance-timeout <minutes>`	Enter the inactivity timeout for compliant endpoints. Range 1 to 480 minutes.	5
`download-location {custom | fortigate | fortiguard}`	Select location from which FortiClient application is downloaded: **`custom`** — set `download-custom-link` to a URL that provides the download **`fortigate`** — this FortiGate unit, available on some models **`fortiguard`** — FortiGuard Services	`fortiguard`
`download-custom-link <url>`	Enter a URL where the FortiClient installer can be downloaded. This is available if `download-location` is `custom`.	No default.
`enforce-minimum-version {enable | disable}`	Enable to require that Endpoints run a version of FortiClient Endpoint Security defined by `version` or `version-check`.	`disable`
`version <major.minor.patch>`	Enter the minimum acceptable version of the FortiClient application. This is available if `version-check` is `minimum`.	`4.0.0`
`version-check {latest | minimum}`	Enter `latest` to require the newest version available from the download location. Enter `minimum` to specify a minimum version in `version`. This is available if `enforce-minimum-version` is enabled.	`minimum`

If `download-location` is `fortiguard` and FortiGuard Services is not available, the download portal directs the user to contact the administrator.

History

FortiOS v4.0 New.

FortiOS v4.0 MR1 Added `compliance-timeout`, `enforce-minimum-version`.

Related commands

- endpoint-control apps-detect rule-list

firewall

Use firewall commands to configure firewall policies and the data they use, including protection profiles, IP addresses and virtual IP addresses, schedules, and services. You can also configure DNS translation, IP/MAC binding, and multicast policies.

This chapter contains the following sections:

address, address6

Use this command to configure firewall addresses used in firewall policies. An IPv4 firewall address is a set of one or more IP addresses, represented as a domain name, an IP address and a subnet mask, or an IP address range. An IPv6 firewall address is an IPv6 6-to-4 address prefix.

By default, FortiGate units have the firewall address All, which represents any IP address.

Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies. If an address is selected in a policy, it cannot be deleted until it is deselected from the policy.

Syntax

```
config firewall address
  edit <name_str>
    set associated-interface <interface_str>
    set cache-ttl <ttl_int>
    set comment <comment_string>
    set end-ip <address_ipv4>
    set fqdn <domainname_str>
    set start-ip <address_ipv4>
    set subnet <address_ipv4mask>
    set type {ipmask | iprange | fqdn | wildcard}
    set wildcard <address_ip4mask>
  end
config firewall address6
  edit <name_str>
    set ip6 <address_ipv6prefix>
  end
```

Variable	Description	Default
The following fields are for `config firewall address`.		
`<name_str>`	Enter the name of the address.	No default.
`associated-interface <interface_str>`	Enter the name of the associated interface. If not configured, the firewall address is bound to an interface during firewall policy configuration.	No default.
`cache-ttl <ttl_int>`	Enter minimum time-to-live (TTL) of individual IP addresses in FQDN cache. This is available when `type` is `fqdn`.	0
`comment <comment_string>`	Enter any comments for this address.	No default.
`end-ip <address_ipv4>`	If `type` is `iprange`, enter the last IP address in the range.	`0.0.0.0`
`fqdn <domainname_str>`	If `type` is `fqdn`, enter the fully qualified domain name (FQDN).	No default.
`start-ip <address_ipv4>`	If `type` is `iprange`, enter the first IP address in the range.	`0.0.0.0`
`subnet <address_ipv4mask>`	If `type` is `ipmask`, enter an IP address then its subnet mask, in dotted decimal format and separated by a space, or in CIDR format with no separation. For example, you could enter either: • `172.168.2.5/32` • `172.168.2.5 255.255.255.255` The IP address can be for a single computer or a subnetwork. The subnet mask corresponds to the class of the IP address being added. • A single computer's subnet mask is `255.255.255.255` or `/32`. • A class A subnet mask is `255.0.0.0` or `/8`. • A class B subnet mask is `255.255.0.0` or `/26`. • A class C subnet mask is `255.255.255.0` or `/24`.	`0.0.0.0` `0.0.0.0`

Variable	Description	Default
`type {ipmask | iprange | fqdn | wildcard}`	Select whether this firewall address is a subnet address, an address range, fully qualified domain name, or an IP with a wildcard netmask.	`ipmask`
`wildcard <address_ip4mask>`	This is available if `type` is `wildcard`.	`0.0.0.0 0.0.0.0`
The following field is for `config firewall address6`.		
`<name_str>`	Enter the name of the IPv6 address prefix.	No default.
`ip6 <address_ipv6prefix>`	If the IP address is IPv6, enter an IPv6 IP address prefix.	`::/0`

Example

This example shows how to add one IPv4 address of each type: `ipmask`, `iprange`, and `fqdn`. It also shows how to configure an IPv6 address prefix.

```
config firewall address
  edit Example_Subnet
    set type ipmask
    set subnet 192.168.1.0 255.255.255.0
  next
  edit Example_Range
    set type iprange
    set start-ip 10.10.1.10
    set end-ip 10.10.1.30
  next
  edit Example_Domain
    set type fqdn
    set fqdn www.example.com
  end

config firewall address6
  edit Example_ipv6_Prefix
    set ip6 2002:CF8E:83CA::/48
  end
```

History

FortiOS v2.80	Substantially revised. IP address range option added. Requiring that an address be added to an interface removed.
FortiOS v3.0	Added `fqdn`.
FortiOS v3.0 MR4	Added `associated-interface` field.
FortiOS v3.0 MR7	Added `wildcard` option to `type`. Allows for firewall address with a wildcard netmask.
FortiOS v4.0	Added `comment` field.
FortiOS v4.0 MR1	Added `cache-ttl` field.

Related topics

- firewall addrgrp, addrgrp6
- firewall policy, policy6

addrgrp, addrgrp6

Use this command to configure firewall address groups used in firewall policies.

You can organize related firewall addresses into firewall address groups to simplify firewall policy configuration. For example, rather than creating three separate firewall policies for three firewall addresses, you could create a firewall address group consisting of the three firewall addresses, then create one firewall policy using that firewall address group.

Addresses, address groups, and virtual IPs must all have unique names to avoid confusion in firewall policies. If an address group is selected in a policy, it cannot be deleted unless it is first deselected in the policy.

Syntax

```
config firewall addrgrp, addrgrp6
  edit <name_str>
    set comment <comment_string>
    set member <name_str>
  end
```

Variable	Description	Default
<name_str>	Enter the name of the address group.	No default.
comment <comment_string>	Enter any comments for this address group.	No default.
member <name_str>	Enter one or more names of firewall addresses to add to the address group. Separate multiple names with a space. To remove an address name from the group, retype the entire new list, omitting the address name.	No default.

Example

This example shows how to add two firewall addresses to a firewall address group.

```
config firewall addrgrp
  edit Group1
    set member Example_Subnet Example_Range
  end
```

History

FortiOS v2.80 Revised.

FortiOS v4.0 Added option comment.

Related topics

- firewall address, address6
- firewall policy, policy6

dnstranslation

Use this command to add, edit or delete a DNS translation entry.

If DNS translation is configured, the FortiGate unit rewrites the payload of outbound DNS query replies from internal DNS servers, replacing the resolved names' internal network IP addresses with external network IP address equivalents, such as a virtual IP address on a FortiGate unit's external network interface. This allows external network hosts to use an internal network DNS server for domain name resolution of hosts located on the internal network.

For example, if a virtual IP provided network address translation (NAT) between a public network, such as the Internet, and a private network containing a web server, hosts on the public network could access the web server by using its virtual IP address. However, if hosts attempted to access the web server by domain name, and the DNS server performing name resolution for that domain name was also located on the private network, the DNS query reply would contain a private network IP address, which is not routable from the external network. To solve this, you might configure DNS translation, and substitute the web server's private network IP address with the virtual IP address in DNS query replies to the public network.

DNS translation mappings between `src` and `dst` must be one-to-one; you cannot create one-to-many or many-to-one mappings. For example, if `src` is a single IP address, it cannot be DNS translated into a `dst` subnet; `dst` must be a single IP address, like `src`. If `src` is a subnet, `dst` must also be a subnet.

Syntax

```
config firewall dnstranslation
  edit <index_int>
    set dst <destination_ipv4>
    set netmask <address_ipv4mask>
    set src <source_ipv4>
  end
```

Variable	Description	Default
`<index_int>`	Enter the unique ID number of the DNS translation entry.	No default.
`dst <destination_ipv4>`	Enter the IP address or subnet on the external network to substitute for the resolved address in DNS query replies. `dst` can be either a single IP address or a subnet on the external network, but must be equal in number to the number of mapped IP addresses in `src`.	`0.0.0.0`
`netmask <address_ipv4mask>`	If `src` and `dst` are subnets rather than single IP addresses, enter the netmask for both `src` and `dst`.	`0.0.0.0`
`src <source_ipv4>`	Enter the IP address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with `dst`.	`0.0.0.0`

Example

This example shows how to translate the resolved addresses in DNS query replies, from an internal (source) subnet to an external (destination) subnet.

```
config firewall dnstranslation
  edit 1
    set src 192.168.100.12
    set dst 172.16.200.190
    set netmask 255.255.255.0
  end
```

History

FortiOS v2.80 Revised.

Related topics

- firewall vip

interface-policy

DoS policies, called interface policies in the CLI, are primarily used to apply DoS sensors to network traffic based on the FortiGate interface it is leaving or entering as well as the source and destination addresses. DoS sensors are a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. A common example of anomalous traffic is the denial of service attack. A denial of service occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system so legitimate users can no longer use it. You can also use the `Interface-policy` command to invoke an IPS sensor as part of a DoS policy.

The `interface-policy` command is used for DoS policies applied to IPv4 addresses. For IPv6 addresses, use `interface-policy6` instead.

Syntax

```
config firewall interface-policy
  edit <policy_id>
    set application-list-status {enable | disable}
    set application_list <app_list_str>
    set dstaddr <dstaddr_ipv4>
    set interface <int_str>
    set ips-DoS-status {enable | disable}
    set ips-DoS <DoS_str>
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set service <service_str>
    set srcaddr <srcaddr_ipv4>
    set status {enable | disable}
end
```

Variable	Description	Default
`application-list-status {enable | disable}`	Enable to have the FortiGate unit apply an application black/white list to matching network traffic.	`disable`
`application_list <app_list_str>`	Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when `application-list-status` is set to `enable`.	
`dstaddr <dstaddr_ipv4>`	Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range.	
`interface <int_str>`	The interface or zone to be monitored.	
`ips-DoS-status {enable | disable}`	Enable to have the FortiGate unit examine network traffic for DoS sensor violations.	`disable`
`ips-DoS <DoS_str>`	Enter the name of the DoS sensor the FortiGate unit will use when examining network traffic. This option is available only when `ips-DoS-status` is set to `enable`.	
`ips-sensor-status {enable | disable}`	Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities.	`disable`
`ips-sensor <sensor_str>`	Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when `ips-sensor-status` is set to `enable`.	

Variable	Description	Default
`service <service_str>`	Enter a service to limit traffic monitoring to only the selected type. You may also specify a service group, or multiple services separated by spaces.	
`srcaddr <srcaddr_ipv4>`	Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range.	
`status {enable | disable}`	Enable or disable the DoS policy. A disabled DoS policy has no effect on network traffic.	`enable`

Example

This example shows how to add a DoS policy that examines all traffic received by port10 with source and destination addresses matching Subnet_1 and Subnet_2 and for any service. The policy applies an IPS sensor to the traffic.

```
config firewall interface-policy
  edit 1
    set interface port10
    set srcaddr Subnet_1
    set dstaddr Subnet_2
    set ips-sensor-status enable
    set ips-sensor mySensor
  end
```

History

FortiOS v4.0 New.

FortiOS v4.0 MR1 Added `application_list` and `application_list_status` fields.

Related commands

- firewall interface-policy6
- firewall sniff-interface-policy
- firewall sniff-interface-policy6
- firewall policy, policy6
- firewall profile

interface-policy6

DoS policies (called interface policies in the CLI) for IPv6 addresses, are used to apply IPS sensors to network traffic based on the FortiGate interface it is leaving or entering as well as the source and destination addresses.

The `interface-policy6` command is used for DoS policies applied to IPv6 addresses. For IPv4 addresses, use `interface-policy` instead.

Syntax

```
config firewall interface-policy6
  edit <policy_id>
    set application-list-status {enable | disable}
    set application_list <app_list_str>
    set dstaddr6 <dstaddr_ipv6>
    set interface
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set service6 <service_str>
    set srcaddr6 <srcaddr_ipv6>
    set status {enable | disable}
end
```

Variable	Description	Default
`application-list-status {enable | disable}`	Enable to have the FortiGate unit apply an application black/white list to matching network traffic.	`disable`
`application_list <app_list_str>`	Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when `application-list-status` is set to `enable`.	
`dstaddr6 <dstaddr_ipv6>`	Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range.	
`interface`	The interface or zone to be monitored.	
`ips-sensor-status {enable | disable}`	Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities.	`disable`
`ips-sensor <sensor_str>`	Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when `ips-sensor-status` is set to `enable`.	
`service6 <service_str>`	Enter a service to limit traffic monitoring to only the selected type. You may also specify a service group, or multiple services separated by spaces.	
`srcaddr6 <srcaddr_ipv6>`	Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range.	
`status {enable | disable}`	Enable or disable the DoS policy. A disabled DoS policy has no effect on network traffic.	`enable`

Example

This example shows how to add an IPv6 sniffer policy that examines all IPv6 traffic received by port10 with source and destination addresses matching Subnet_1 and Subnet_2 and for any service. The policy applies an application control list and an IPS sensor to the traffic.

```
config firewall interface-policy6
  edit 1
```

```
    set interface port10
    set srcaddr Subnet_1
    set dstaddr Subnet_2
    set service ANY
    set ips-sensor-status enable
    set ips-sensor mySensor
  end
```

History

FortiOS v4.0	New.
FortiOS v4.0 MR1	Added `application_list` and `application_list_status` fields.

Related commands

- firewall interface-policy
- firewall sniff-interface-policy
- firewall sniff-interface-policy6
- firewall policy, policy6
- firewall profile

ipmacbinding setting

Use this command to configure IP to MAC address binding settings.

IP/MAC binding protects the FortiGate unit and/or the network from IP address spoofing attacks. IP spoofing attacks attempt to use the IP address of a trusted computer to connect to, or through, the FortiGate unit from a different computer. It is simple to change a computer's IP address to mimic that of a trusted host, but MAC addresses are often added to Ethernet cards at the factory, and are more difficult to change. By requiring that traffic from trusted hosts reflect both the IP address and MAC address known for that host, fraudulent connections are more difficult to construct.

To configure the table of IP addresses and the MAC addresses bound to them, see "ipmacbinding table" on page 121. To enable or disable IP/MAC binding for an individual FortiGate unit network interface, see `ipmac` in "system interface" on page 448.

Note: If IP/MAC binding is enabled, and the IP address of a host with an IP or MAC address in the IP/MAC table is changed, or a new computer is added to the network, update the IP/MAC table. If you do not update the IP/MAC binding list, the new or changed hosts will not have access to or through the FortiGate unit. For details on updating the IP/MAC binding table, see "ipmacbinding table" on page 121.

Caution: If a client receives an IP address from the FortiGate unit's DHCP server, the client's MAC address is automatically registered in the IP/MAC binding table. This can simplify IP/MAC binding configuration, but can also neutralize protection offered by IP/MAC binding if untrusted hosts are allowed to access the DHCP server. Use caution when enabling and providing access to the DHCP server.

Syntax

```
config firewall ipmacbinding setting
  set bindthroughfw {enable | disable}
  set bindtofw {enable | disable}
  set undefinedhost {allow | block}
end
```

Variable	Description	Default
`bindthroughfw {enable | disable}`	Select to use IP/MAC binding to filter packets that a firewall policy would normally allow ***through*** the FortiGate unit.	`disable`
`bindtofw {enable | disable}`	Select to use IP/MAC binding to filter packets that would normally connect ***to*** the FortiGate unit.	`disable`
`undefinedhost {allow | block}`	Select how IP/MAC binding handles packets with IP and MAC addresses that are not defined in the IP/MAC list for traffic going through or to the FortiGate unit. • `allow`: Allow packets with IP and MAC address pairs that are not in the IP/MAC binding list. • `block`: Block packets with IP and MAC address pairs that are not in the IP/MAC binding list. This option is available only when either or both `bindthroughfw` and `bindtofw` are `enable`.	`block`

Example

This example shows how to enable IP/MAC binding for traffic both going to and through the FortiGate unit, and block undefined hosts (IP/MAC address pairs).

```
config firewall ipmacbinding setting
  set bindthroughfw enable
  set bindtofw enable
  set undefinedhost block
end
```

History

FortiOS v2.80 Revised.

Related topics

- firewall ipmacbinding table

ipmacbinding table

Use this command to configure IP and MAC address pairs in the IP/MAC binding table. You can bind multiple IP addresses to the same MAC address, but you cannot bind multiple MAC addresses to the same IP address.

To configure the IP/MAC binding settings, see "ipmacbinding setting" on page 119. To enable or disable IP/MAC binding for an individual FortiGate unit network interface, see `ipmac` in "system interface" on page 448.

Note: If IP/MAC binding is enabled, and the IP address of a host with an IP or MAC address in the IP/MAC table is changed, or a new computer is added to the network, update the IP/MAC table. If you do not update the IP/MAC binding list, the new or changed hosts will not have access to or through the FortiGate unit.

Caution: If a client receives an IP address from the FortiGate unit's DHCP server, the client's MAC address is automatically registered in the IP/MAC binding table. This can simplify IP/MAC binding configuration, but can also neutralize protection offered by IP/MAC binding if untrusted hosts are allowed to access the DHCP server. Use caution when enabling and providing access to the DHCP server.

Syntax

```
config firewall ipmacbinding table
  edit <index_int>
    set ip <address_ipv4>
    set mac <address_hex>
    set name <name_str>
    set status {enable | disable}
  end
```

Variable	Description	Default
`<index_int>`	Enter the unique ID number of this IP/MAC pair.	No default.
`ip <address_ipv4>`	Enter the IP address to bind to the MAC address. To allow all packets with the MAC address, regardless of the IP address, set the IP address to `0.0.0.0`.	`0.0.0.0`
`mac <address_hex>`	Enter the MAC address. To allow all packets with the IP address, regardless of the MAC address, set the MAC address to `00:00:00:00:00:00`.	`00:00:00:00:00:00`
`name <name_str>`	Enter a name for this entry on the IP/MAC address table. (Optional.)	`noname`
`status {enable | disable}`	Select to enable this IP/MAC address pair. Packets not matching any IP/MAC binding will be dropped. Packets matching an IP/MAC binding will be matched against the firewall policy list.	`disable`

Example

This example shows how to add and enable an IP/MAC entry to the IP/MAC binding table.

```
config firewall ipmacbinding table
  edit 1
    set ip 172.16.44.55
    set mac 00:10:F3:04:7A:4C
    set name RemoteAdmin
    set status enable
  end
```

History

FortiOS v2.80 Revised.

Related topics

- firewall ipmacbinding setting

ippool

Use this command to configure IP address pools.

Use IP pools to add NAT policies that translate source addresses to addresses randomly selected from the IP pool, rather than the IP address assigned to that FortiGate unit interface. In Transparent mode, IP pools are available only from the FortiGate CLI.

An IP pool defines a single IP address or a range of IP addresses. A single IP address in an IP pool becomes a range of one IP address. For example, if you enter an IP pool as 1.1.1.1 the IP pool is actually the address range 1.1.1.1 to 1.1.1.1.

If a FortiGate interface IP address overlaps with one or more IP pool address ranges, the interface responds to ARP requests for all of the IP addresses in the overlapping IP pools.

For example, consider a FortiGate unit with the following IP addresses for the port1 and port2 interfaces:

- port1 IP address: 1.1.1.1/255.255.255.0 (range is 1.1.1.0-1.1.1.255)
- port2 IP address: 2.2.2.2/255.255.255.0 (range is 2.2.2.0-2.2.2.255)

And the following IP pools:

- IP_pool_1: 1.1.1.10-1.1.1.20
- IP_pool_2: 2.2.2.10-2.2.2.20
- IP_pool_3: 2.2.2.30-2.2.2.40

The port1 interface overlap IP range with IP_pool_1 is:

- (1.1.1.0-1.1.1.255) and (1.1.1.10-1.1.1.20) = 1.1.1.10-1.1.1.20

The port2 interface overlap IP range with IP_pool_2 is:

- (2.2.2.0-2.2.2.255) & (2.2.2.10-2.2.2.20) = 2.2.2.10-2.2.2.20

The port2 interface overlap IP range with IP_pool_3 is:

- (2.2.2.0-2.2.2.255) & (2.2.2.30-2.2.2.40) = 2.2.2.30-2.2.2.40

And the result is:

- The port1 interface answers ARP requests for 1.1.1.10-1.1.1.20
- The port2 interface answers ARP requests for 2.2.2.10-2.2.2.20 and for 2.2.2.30-2.2.2.40

Select *NAT* in a firewall policy and then select *Dynamic IP Pool* and select an IP pool to translate the source address of packets leaving the FortiGate unit to an address randomly selected from the IP pool.

Syntax

```
config firewall ippool
  edit <index_int>
    set endip <address_ipv4>
    set startip <address_ipv4>
  end
```

Variable	Description	Default
`<index_int>`	The unique ID number of this IP pool.	No default.
`endip <address_ipv4>`	The end IP of the address range. The end IP must be higher than the start IP. The end IP does not have to be on the same subnet as the IP address of the interface for which you are adding the IP pool.	0.0.0.0
`startip <address_ipv4>`	The start IP of the address range. The start IP does not have to be on the same subnet as the IP address of the interface for which you are adding the IP pool.	0.0.0.0

Example

You can use the following commands to add an IP pool.

```
config firewall ippool
  edit 1
    set startip 192.168.1.100
    set endip 192.168.1.200
  end
```

History

FortiOS v2.80 Revised.

FortiOS v4.0 MR1 `interface` field removed.

Related topics

- firewall policy, policy6

ldb-monitor

Use this command to configure health check settings.

Health check settings can be used by load balancing VIPs to determine if a real server is currently responsive before forwarding traffic. One health check is sent per interval using the specified protocol, port and HTTP-GET, where applicable to the protocol. If the server does not respond during the timeout period, the health check fails and, if retries are configured, another health check is performed. If all health checks fail, the server is deemed unavailable, and another real server is selected to receive the traffic according to the selected load balancing algorithm.

Health check settings can be re-used by multiple real servers. For details on enabling health checking and using configured health check settings, see “firewall vip” on page 189.

Syntax

```
config firewall ldb-monitor
  edit <name_str>
    set http-get <httprequest_str>
    set http-match <contentmatch_str>
    set interval <seconds_int>
    set port <port_int>
    set retry <retries_int>
    set timeout <seconds_int>
    set type {http | ping | tcp}
  end
```

Variable	Description	Default
<name_str>	Enter the name of the health check monitor.	No default.
http-get <httprequest_str>	For HTTP health check monitors, add a URL that the FortiGate unit uses when sending a get request to check the health of a HTTP server. The URL should match an actual URL for the real HTTP servers. The URL is optional. The URL would not usually include an IP address or domain name. Instead it should start with a /and be followed by the address of an actual web page on the real server. For example, if the IP address of the real server is 10.10.10.1, the URL /test_page.htm causes the FortiGate unit to send am HTTP get request to http://10.10.10.1/test_page.htm. This option appears only if type is http.	No default.
http-match <contentmatch_str>	For HTTP health check monitors, add a phrase that a real HTTP server should include in response to the get request sent by the FortiGate unit using the content of the http-get option. If the http-get URL returns a web page, the http-match option should exactly match some of the text on the web page. You can use the http-get and http-matched options to verify that an HTTP server is actually operating correctly by responding to get requests with expected web pages. http-match is only required if you add a http-get URL. For example, you can set http-match to “server test page” if the real HTTP server page defined by http-get contains the phrase server test page. When the FortiGate unit receives the web page in response to the URL get request, the system searches the content of the web page for the http-match phrase. This option appears only if type is http.	No default.
interval <seconds_int>	Enter the interval time in seconds between health checks.	10

Variable	Description	Default
`port <port_int>`	Enter the port number used to perform the health check. If you set the `Port` to `0`, the health check monitor uses the port defined in the real server. This way you can use a single health check monitor for different real servers. This option does not appear if `type` is `ping`.	0
`retry <retries_int>`	Enter the number of times that the FortiGate unit should retry the health check if a health check fails. If all health checks, including retries, fail, the server is deemed unavailable.	3
`timeout <seconds_int>`	Enter the timeout in seconds. If the FortiGate unit does not receive a response to the health check in this period of time, the health check fails.	2
`type {http | ping | tcp}`	Select the protocol used by the health check monitor.	No default.

Example

You might configure a health check for a server using the HTTP protocol to retrieve a web page. To ensure that a web page reply containing an error message, such as an HTTP 404 page, does not inadvertently cause the health check to succeed, you might search the reply for text that does not occur in any web server error page, such as unique text on a main page.

```
config firewall ldp-monitor
  edit httphealthchecksettings
    set type http
    set port 8080
    set http-get “/index.php”
    set http-match “Welcome to Example, Inc.”
    set interval 5
    set timeout 2
    set retry 2
  end
```

History

FortiOS v3.0 MR6 New command. Configures health check settings which can be used when enabling health checks for load balanced real servers associated with a virtual IP. This extends and replaces deprecated commands in `config realserver` for health check by ICMP ECHO (ping).

Related topics

- firewall vip

multicast-policy

Use this command to configure a source NAT IP. This command can also be used in Transparent mode to enable multicast forwarding by adding a multicast policy.

The matched forwarded (outgoing) IP multicast source IP address is translated to the configured IP address. For additional options related to multicast, see multicast-forward {enable | disable} in "system settings" on page 517 and tp-mc-skip-policy {enable | disable} in "system global" on page 423.

Syntax

```
config firewall multicast-policy
  edit <index_int>
    set action {accept | deny}
    set dnat <address_ipv4>
    set dstaddr <address_ipv4mask>
    set dstintf <name_str>
    set nat <address_ipv4>
    set srcaddr <address_ipv4mask>
    set srcintf <name_str>
    set protocol <multicastlimit_int>
    set start-port <port_int>
    set end-port <port_int>
  end
```

Variable	Description	Default
<index_int>	Enter the unique ID number of this multicast policy.	No default.
action {accept | deny}	Enter the policy action.	accept
dnat <address_ipv4>	Enter an IP address to destination network address translate (DNAT) externally received multicast destination addresses to addresses that conform to your organization's internal addressing policy.	0.0.0.0
dstaddr <address_ipv4mask>	Enter the destination IP address and netmask, separated by a space, to match against multicast NAT packets.	0.0.0.0 0.0.0.0
dstintf <name_str>	Enter the destination interface name to match against multicast NAT packets.	No default.
nat <address_ipv4>	Enter the IP address to substitute for the original source IP address.	0.0.0.0
srcaddr <address_ipv4mask>	Enter the source IP address and netmask to match against multicast NAT packets.	0.0.0.0 0.0.0.0
srcintf <name_str>	Enter the source interface name to match against multicast NAT packets.	No default.
protocol <multicastlimit_int>	Limit the number of protocols (services) sent out via multicast using the FortiGate unit.	0
start-port <port_int>	The beginning of the port range used for multicast.	No default.
end-port <port_int>	The end of the port range used for multicast.	65535

Example

This example shows how to configure a multicast NAT policy.

```
config firewall multicast-policy
  edit 1
    set dstaddr 10.0.0.1 255.255.255.0
    set dstintf dmz
```

```
    set nat 10.0.1.1
    set srcaddr 192.168.100.12 255.255.255.0
    set srcintf internal
  end
```

History

FortiOS v2.80	Revised.
FortiOS v3.0 MR4	Added `protocol`, `start-port`, and `end-port` to `multicast-policy`.
FortiOS v3.0 MR5	Added `dnat`.

Related topics

- system global

policy, policy6

Use this command to add, edit, or delete firewall policies.

Firewall policies control all traffic passing through the FortiGate unit. Firewall policies are instructions used by the FortiGate unit to decide what to do with a connection request. The policy directs the firewall to allow the connection, deny the connection, require authentication before the connection is allowed, or apply IPSec or SSL VPN processing.

Note: If you are creating an IPv6 policy, some of the IPv4 options, such as NAT and VPN settings, are not applicable.

Syntax

```
config firewall policy, policy6
  edit <index_int>
    set action {accept | deny | ipsec | ssl-vpn}
    set auth-cert <certificate_str>
    set auth-path {enable | disable}
    set auth-redirect-addr <domainname_str>
    set comments <comment_str>
    set custom-log-fields <fieldid_int>
    set diffserv-forward {enable | disable}
    set diffserv-reverse {enable | disable}
    set diffservcode-forward <dscp_bin>
    set diffservcode-rev <dscp_bin>
    set disclaimer {enable | disable}
    set dstaddr <name_str>
    set dstintf <name_str>
    set fixedport {enable | disable}
    set endpoint-check {enable | disable}
    set endpoint-profile <ep_profile_name>
    set fsae {enable | disable}
    set fsae-guest-profile <profile_str>
    set fsae-server-for-ntlm <server_str>
    set identity-based {enable | disable}
    set inbound {enable | disable}
    set ippool {enable | disable}
    set logtraffic {enable | disable}
    set match-vip {enable | disable}
    set nat {enable | disable}
    set natinbound {enable | disable}
    set natip <address_ipv4mask>
    set natoutbound {enable | disable}
    set ntlm {enable | disable}
    set outbound {enable | disable}
    set per-ip-shaper <shaper_name>
    set poolname <name_str>
    set profile <name_str>
    set profile-status {enable | disable}
    set redirect-url <name_str>
    set schedule <name_str>
    set service <name_str>
    set session-ttl <session_time_integer>
```

```
    set srcaddr <name_str>
    set srcintf <name_str>
    set sslvpn-auth {any | ldap | local | radius | tacacs+}
    set sslvpn-ccert {enable | disable}
    set sslvpn-cipher {0 | 1 | 2}
    set status {enable | disable}
    set tcp-mss-sender <maximumsize_int>
    set tcp-mss-receiver <maximumsize_int>
    set traffic-shaper <name_str>
    set traffic-shaper-reverse <name_str>
    set vpntunnel <name_str>
    set wccp {enable | disable}
    config identity-based-policy
      edit <policy_id>
        set groups <group_name>
        set logtraffic {enable | disable}
        set profile <name_str>
        set schedule <name_str>
        set service <name_str>
        set traffic-shaper <name_str>
        set traffic-shaper-reverse <name_str>
        end
      end
  end
```

Variable	Description	Default
<index_int>	Enter the unique ID number of this policy.	No default.
action {accept | deny | ipsec | ssl-vpn}	Select the action that the FortiGate unit will perform on traffic matching this firewall policy. • accept: Allow packets that match the firewall policy. Also enable or disable nat to make this a NAT policy (NAT/Route mode only), enable or disable ippool so that the NAT policy selects a source address for packets from a pool of IP addresses added to the destination interface, and enable or disable fixedport so that the NAT policy does not translate the packet source port. • deny: Deny packets that match the firewall policy. • ipsec: Allow and apply IPSec VPN. When action is set to ipsec, you must specify the vpntunnel attribute. You may also enable or disable the inbound, outbound, natoutbound, and natinbound attributes and/or specify a natip value. • ssl-vpn: Allow and apply SSL VPN. When action is set to ssl-vpn, you may specify values for the sslvpn-auth, sslvpn-ccert, and sslvpn-cipher attributes. For IPv6 policies, only accept and deny options are available.	deny
auth-cert <certificate_str>	Select a HTTPS server certificate for policy authentication. self-sign is the built-in, self-signed certificate; if you have added other certificates, you may select them instead. This option appears only if identity-based is enable.	No default.

Variable	Description	Default
`auth-path {enable | disable}`	Select to apply authentication-based routing. You must also specify a RADIUS server, and the RADIUS server must be configured to supply the name of an object specified in `config router auth-path`. For details on configuring authentication-based routes, see "router auth-path" on page 281. This option appears only when the FortiGate unit is operating in NAT mode and `identity-based` is `enable`. For details on NAT and transparent mode, see "opmode {nat | transparent}" on page 519.	`disable`
`auth-redirect-addr <domainname_str>`	Enter the IP address or domain name to redirect user HTTP requests after accepting the authentication disclaimer. The redirect URL could be to a web page with extra information (for example, terms of usage). To prevent web browser security warnings, this should match the CN field of the specified `auth-cert`, which is usually a fully qualified domain name (FQDN). This option appears only if `identity-based` is `enable`.	No default.
`comments <comment_str>`	Enter a description or other information about the policy. (Optional) `comment_str` is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces. For more information, see "Special characters" on page 46.	No default.
`custom-log-fields <fieldid_int>`	Enter custom log field index numbers to append one or more custom log fields to the log message for this policy. Separate multiple log custom log field indices with a space. (Optional.) This option takes effect only if logging is enabled for the policy, and requires that you first define custom log fields. For details, see "log custom-field" on page 234.	No default.
`diffserv-forward {enable | disable}`	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure `diffservcode-forward`.	`disable`
`diffserv-reverse {enable | disable}`	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of reverse (reply) traffic. If enabled, also configure `diffservcode-rev`.	`disable`
`diffservcode-forward <dscp_bin>`	Enter the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if `diffserv-forward` is `enable`. For details and DSCP configuration examples, see the Knowledge Center article Differentiated Services Code Point (DSCP) behavior.	`000000`
`diffservcode-rev <dscp_bin>`	Enter the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if `diffserv-rev` is `enable` For details and DSCP configuration examples, see the Knowledge Center article Differentiated Services Code Point (DSCP) behavior.	`000000`
`disclaimer {enable | disable}`	Enable to display the authentication disclaimer page, which is configured with other replacement messages. The user must accept the disclaimer to connect to the destination. This option appears only if `profile` or `groups` (authentication) is configured, and only appears on some models.	`disable`

Variable	Description	Default
`dstaddr <name_str>`	Enter one or more destination firewall addresses, or a virtual IP, if creating a NAT policy. Separate multiple firewall addresses with a space. If `action` is set to `ipsec`, enter the name of the IP address to which IP packets may be delivered at the remote end of the IPSec VPN tunnel. For details, see "Defining IP source and destination addresses" in the *FortiGate IPSec VPN User Guide*. If `action` is set to `ssl-vpn`, enter the name of the IP address that corresponds to the host, server, or network that remote clients need to access behind the FortiGate unit. For details on configuring virtual IPs, see "vip" on page 189.	No default.
`dstintf <name_str>`	Enter the destination interface for the policy. The interface can be a physical interface, a VLAN subinterface, or a zone. If `action` is set to `ipsec`, enter the name of the interface to the external (public) network. If `action` is set to `ssl-vpn`, enter the name of the interface to the local (private) network. **Note:** If a interface or VLAN subinterface has been added to a zone, the interface or VLAN subinterface `cannot be used` for `dstintf`.	No default.
`fixedport {enable | disable}`	Enable to preserve packets' source port number, which may otherwise be changed by a NAT policy. Some applications do not function correctly if the source port number is changed, and may require this option. If `fixedport` is `enable`, you should usually also enable IP pools; if you do not configure an IP pool for the policy, only one connection can occur at a time for this port.	`disable`
`endpoint-check {enable | disable}`	Enable to perform endpoint NAC compliance check. This check denies access to this firewall policy for hosts that do not have up-to-date FortiClient Endpoint Security software running. You need to also configure `endpoint-profile`. **Note:** If the firewall policy involves a load balancing virtual IP, the endpoint compliance check is not performed. For more information, see "endpoint-control" on page 103.	disable
`endpoint-profile <ep_profile_name>`	Select the endpoint NAC profile to apply. This is available when `endpoint-check` is enabled. For information about creating endpoint NAC profiles, see "endpoint-control profile" on page 105.	No default.
`fsae {enable | disable}`	Enable or disable Directory Service authentication. If you enable this option, you must also define the user groups and the guest account protection profile. For details, see "fsae-guest-profile <profile_str>" on page 132 and "groups <group_name>" on page 135.	disable
`fsae-guest-profile <profile_str>`	Enter the name of the protection profile used when a guest account authenticates using FSAE. If any other authentication method is selected in the firewall policy, the fsae guest profile is not applied.	No default.
`fsae-server-for-ntlm <server_str>`	Restrict NTLM authentication to one particular server only for this policy. Enter the name of a server defined in user fsae.	No default.
`identity-based {enable | disable}`	Select to enable or disable identity-based policy authentication. This option appears only if `action` is `accept`.	`disable`
`inbound {enable | disable}`	When `action` is set to `ipsec`, enable or disable traffic from computers on the remote private network to initiate an IPSec VPN tunnel.	`disable`
`ippool {enable | disable}`	When the action is set to accept and NAT is enabled, configure a NAT policy to translate the source address to an address randomly selected from the first IP pool added to the destination interface of the policy.	`disable`
`logtraffic {enable | disable}`	Enable or disable recording traffic log messages for this policy.	`disable`

Variable	Description	Default
match-vip {enable | disable}	The FortiGate unit will check whether DNATed traffic matches the policy if match-vip is enabled. Normally, the FortiGate unit only checks whether DNATed traffic matches VIP policies.	disable
nat {enable | disable}	Enable or disable network address translation (NAT). NAT translates the address and the port of packets accepted by the policy. When NAT is enabled, ippool and fixedport can also be enabled or disabled. FortiOS v3.0 also supports NAT in transparent mode. For details see "Example: Adding a NAT firewall policy in transparent mode" on page 136. This option appears only if action is accept or ssl-vpn.	disable
natinbound {enable | disable}	Enable or disable translating the source addresses IP packets emerging from the tunnel into the IP address of the FortiGate unit's network interface to the local private network. This option appears only if action is ipsec.	disable
natip <address_ipv4mask>	When action is set to ipsec and natoutbound is enabled, specify the source IP address and subnet mask to apply to outbound clear text packets before they are sent through the tunnel. If you do not specify a natip value when natoutbound is enabled, the source addresses of outbound encrypted packets are translated into the IP address of the FortiGate unit's external interface. When a natip value is specified, the FortiGate unit uses a static subnetwork-to-subnetwork mapping scheme to translate the source addresses of outbound IP packets into corresponding IP addresses on the subnetwork that you specify. For example, if the source address in the firewall encryption policy is 192.168.1.0/24 and the natip value is 172.16.2.0/24, a source address of 192.168.1.7 will be translated to 172.16.2.7.	0.0.0.0 0.0.0.0
natoutbound {enable | disable}	When action is set to ipsec, enable or disable translating the source addresses of outbound encrypted packets into the IP address of the FortiGate unit's outbound interface. Enable this attribute in combination with the natip attribute to change the source addresses of IP packets before they go into the tunnel.	disable
ntlm {enable | disable}	Enable or disable Directory Service authentication via NTLM. If you enable this option, you must also define the user groups. For details, see "groups <group_name>" on page 135. This option appears only if identity-based is enable.	disable
outbound {enable | disable}	When action is set to ipsec, enable or disable traffic from computers on the local private network to initiate an IPSec VPN tunnel.	disable
per-ip-shaper <shaper_name>	Enter the name of the per-IP traffic shaper to apply. For information about per-IP traffic shapers, see firewall shaper per-ip-shaper.	No default.
poolname <name_str>	Enter the name of the IP pool. This variable appears only if nat and ippool are enable.	No default.
profile <name_str>	Enter the name of a protection profile to use with the policy. This option appears only if profile-status is enable.	No default.
profile-status {enable | disable}	Enable or disable using a protection profile with the policy. If enabled, also configure profile. This is automatically disabled if a user group with an associated protection profile has been configured in groups. In that case, the protection profile is determined by the user group, rather than the firewall policy.	disable
redirect-url <name_str>	Enter a URL, if any, that the user is redirected to after authenticating and/or accepting the user authentication disclaimer. This option is available on some models, and only appears if disclaimer is enable.	No default.
schedule <name_str>	Enter the name of the one-time or recurring schedule or schedule group to use for the policy.	No default.

Variable	Description	Default
service <name_str>	Enter the name of one or more services, or a service group, to match with the firewall policy. Separate multiple services with a space.	No default.
session-ttl <session_time_integer>	Set the timeout value in the policy to override the global timeout setting defined by using config sys session-ttl. When it is on default value, it will not take effect.	0
srcaddr <name_str>	Enter one or more source firewall addresses for the policy. Separate multiple firewall addresses with a space. If action is set to ipsec, enter the private IP address of the host, server, or network behind the FortiGate unit. If action is set to ssl-vpn and the firewall encryption policy is for web-only mode clients, type all. If action is set to ssl-vpn and the firewall encryption policy is for tunnel mode clients, enter the name of the IP address range that you reserved for tunnel mode clients. To define an address range for tunnel mode clients, see "ssl settings" on page 622.	No default.
srcintf <name_str>	Enter the source interface for the policy. The interface can be a physical interface, a VLAN subinterface or a zone. If the interface or VLAN subinterface has been added to a zone, interface or VLAN subinterface cannot be used for srcintf. If action is set to ipsec, enter the name of the interface to the local (private) network. If action is set to ssl-vpn, enter the name of the interface that accepts connections from remote clients.	No default.
sslvpn-auth {any | ldap | local | radius | tacacs+}	If action is set to ssl-vpn, enter one of the following client authentication options: • If you want the FortiGate unit to authenticate remote clients using any local user group, a RADIUS server, or LDAP server, type any. • If the user group is a local user group, type local. • If the remote clients are authenticated by an external RADIUS server, type radius. • If the remote clients are authenticated by an external LDAP server, type ldap. • If the remote clients are authenticated by an external TACACS+ server, type tacacs+. You must also set the name of the group which will use the authentication method. For details, see "groups <group_name>" on page 135.	any
sslvpn-ccert {enable | disable}	If action is set to ssl-vpn, enable or disable the use of security certificates to authenticate remote clients.	disable
sslvpn-cipher {0 | 1 | 2}	If action is set to ssl-vpn, enter one of the following options to determine the level of SSL encryption to use. The web browser on the remote client must be capable of matching the level that you select: • To use any cipher suite, type 0. • To use a 164-bit or greater cipher suite (high), type 1. • To use a 128-bit or greater cipher suite (medium), type 2.	0
status {enable | disable}	Enable or disable the policy.	enable

Variable	Description	Default
`tcp-mss-sender <maximumsize_int>`	Enter a TCP Maximum Sending Size number for the sender. When a FortiGate unit is configured to use PPPoE to connect to an ISP, certain web sites may not be accessible to users. This occurs because a PPPoE frame takes an extra 8 bytes off the standard Ethernet MTU of 1500. When the server sends the large packet with DF bit set to 1, the ADSL provider's router either does not send an "ICMP fragmentation needed" packet or the packet is dropped along the path to the web server. In either case, the web server never knows fragmentation is required to reach the client. In this case, configure the `tcp-mss-sender` option to enable access to all web sites. For more information, see the article Cannot view some web sites when using PPPoE on the Fortinet Knowledge Center.	`0`
`tcp-mss-receiver <maximumsize_int>`	Enter a TCP MSS number for the receiver.	`0`
`traffic-shaper <name_str>`	Select a traffic shaper for the policy. A traffic shaper controls the bandwidth available to, and sets the priority of the traffic processed by, the policy. This option appears only if `identity-based` is `disable`.	No default.
`traffic-shaper-reverse <name_str>`	Select a reverse traffic shaper. For example, if the traffic direction that a policy controls is from port1 to port2, select this option will also apply the policy shaping configuration to traffic from port2 to port1. This option appears only if a `traffic-shaper` is selected.	No default.
`vpntunnel <name_str>`	Enter the name of a Phase 1 IPSec VPN configuration to apply to the tunnel. This option appears only if `action` is `ipsec`.	No default.
`wccp {enable | disable}`	Enable or disable web cache on the policy. If enabled, the FortiGate unit will check the learned web cache information, and may redirect the traffic to the web cache server.	`disable`
`identity-based-policy`	Create an identity-based firewall policy that requires authentication. This option is only available if `set identity-based` is `enable`. For more information, see identity-based {enable | disable}.	No default.
`<policy_id>`	Enter the name for the identity-based policy.	No default.
`groups <group_name>`	Enter the user group name for the identity-based policy.	No default.
`logtraffic {enable | disable}`	Enable or disable traffic logging for the identity-based policy.	disable
`profile <name_str>`	Enter the protection profile name for the identity-based policy.	No default.
`schedule <name_str>`	Enter the firewall schedule for the identity-based policy.	No default.
`service <name_str>`	Enter the firewall service for the identity-based policy.	No default.
`traffic-shaper <name_str>`	Enter the traffic shaper for the identity-based policy.	No default.
`traffic-shaper-reverse <name_str>`	Enter the reverse direction traffic shaper for the identity-based policy. This option is only available if you have selected a traffic shaper.	No default.

Example: Adding a firewall policy in NAT/Route mode

On a FortiGate-100, FortiGate-200, or FortiGate-300, use the following example to add policy number 2 that allows users on the external network to access a web server on a DMZ network. The policy:

- Is for connections from the external interface (`srcintf` is `external`) to the DMZ interface (`dstintf` is `dmz`)
- Is enabled
- Allows users from any IP address on the Internet to access the web server (`srcaddr` is `all`)

- Allows access to an address on the DMZ network (`dstaddr` is `dmz_web_server`)
- Sets the `schedule` to `Always` so that users can access the web server 24 hours a day, seven days a week
- Sets the `service` to `HTTP` to limit access to the web server to HTTP connections
- Sets `action` to `accept` to allow connections
- Applies network address translation (`nat` is enabled)

```
config firewall policy
  edit 2
    set srcintf external
    set dstintf dmz
    set status enable
    set srcaddr all
    set dstaddr dmz_web_server
    set schedule Always
    set service HTTP
    set action accept
    set nat enable
  end
```

Example: Adding a NAT firewall policy in transparent mode

For NAT firewall policies to work in NAT/Route mode you must have two interfaces on two different networks with two different subnet addresses. Then you can create firewall policies to translate source or destination addresses for packets as they are relayed by the FortiGate unit from one interface to the other.

A FortiGate unit operating in Transparent mode normally has only one IP address, the management IP. To support NAT in Transparent mode you can add a second management IP. These two management IPs must be on different subnets. When you add two management IP addresses, all FortiGate unit network interfaces will respond to connections to both of these IP addresses.

In the example below, all of the PCs on the internal network (subnet address 192.168.1.0/24) are configured with 192.168.1.99 as their default route. One of the management IPs of the FortiGate unit is set to 192.168.1.99. This configuration results in a typical NAT mode firewall. When a PC on the internal network attempts to connect to the Internet, the PC's default route sends packets destined for the Internet to the FortiGate unit internal interface.

Similarly on the DMZ network (subnet address 10.1.1.0/24) all of the PCs have a default route of 10.1.1.99.

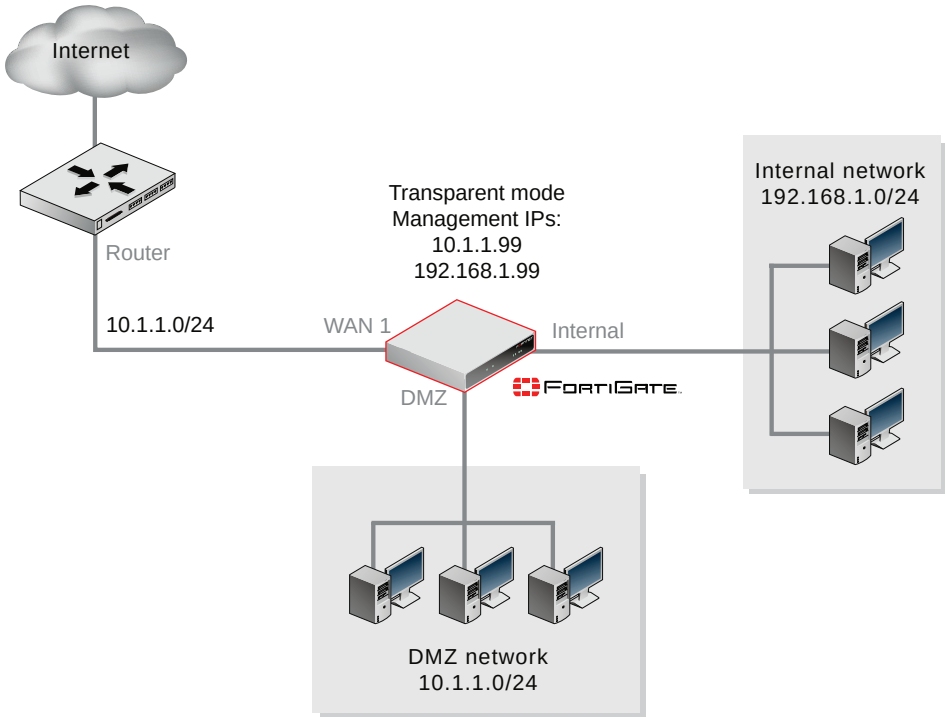
The example describes adding an internal to wan1 firewall policy to relay these packets from the internal interface out the wan1 interface to the Internet. Because the wan1 interface does not have an IP address of its own, you must add an IP pool that translates the source addresses of the outgoing packets to an IP address on the network connected to the wan1 interface.

The example describes adding an IP pool with a single IP address of 10.1.1.201. So all packets sent by a PC on the internal network that are accepted by the internal to wan1 policy leave the wan1 interface with their source address translated to 10.1.1.201. These packets can now travel across the Internet to their destination. Reply packets return to the wan1 interface because they have a destination address of 10.1.1.201. The internal to wan1 NAT policy translates the destination address of these return packets to the IP address of the originating PC and sends them out the internal interface to the originating PC.

Use the following steps to configure NAT in Transparent mode

- Adding two management IPs
- Adding an IP pool
- Adding an internal to wan1 firewall policy

Figure 4: Example NAT in Transparent mode configuration



To add a source address translation NAT policy in Transparent mode

1 Enter the following command to add two management IPs.

The second management IP is the default gateway for the internal network.

```
config system settings
  set manageip 10.1.1.99/24 192.168.1.99/24
end
```

2 Enter the following command to add an IP pool:

```
config firewall ippool
  edit nat-out
    set startip 10.1.1.201
    set endip 10.1.1.201
  end
```

3 Enter the following command to add an internal to wan1 firewall policy with NAT enabled that also includes an IP pool:

```
config firewall policy
  edit 1
    set srcintf "internal"
    set dstintf "wan1"
    set scraddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
    set ippool enable
    set poolname nat-out
  end
```

Note: You can add the firewall policy from the web-based manager and then use the CLI to enable NAT and add the IP Pool.

History

FortiOS v2.80	Revised.
FortiOS v2.80 MR2	Replaced `usrgrp` field with `userdomain`. Added `poolname` field.
FortiOS v2.80 MR3	Removed `userdomain` field. Added `groups` field.
FortiOS v2.80 MR6	Removed `authentication` field. Authentication is automatically enabled for a policy when one or more user group are set with the `groups` field.
FortiOS v3.0	Added `ssl-vpn` options: sslvpn-ccert, sslvpn-cipher, and sslvpn-auth. The `encrypt` action name changed to `ipsec`. Updated `ipsec` options: `vpntunnel`, `inbound`, `outbound`, `natoutbound`, `natinbound`, and `natip`. Added `fsae`. Changes to `profile` and `profile_status`. Added `tcp-mms-sender` and `tcp-mss-receiver`.
FortiOS v3.0 MR4	Added the command `ntlm`. Described the new ability to add multiple entries for the following commands: `srcaddr`, `dstaddr`, and `service`. Nat policy in transparent mode example added.
FortiOS v3.0 MR5	Added `secure-vlan` field. This is available only on the FortiGate-224B unit.
FortiOS v3.0 MR6	New variable `custom-log-fields <fieldid_int>`. Selects custom log fields to append to the policy's log message.
FortiOS v3.0 MR6	New option `tacacs+`. Selects TACACS+ authentication method when the firewall policy `action` is set to `ssl-vpn`.
FortiOS v3.0 MR6	New variable `auth-path {enable | disable}`. Enables or disables authentication-based routing.
FortiOS v3.0 MR6	New variable `auth-redirect-addr <domainname_str>`. Specifies address used in URL when performing HTTP-to-HTTPS redirects for policy authentication.
FortiOS v4.0.0	Removed fields `forticlient-check, forticlient-ra-db-outdated, forticlient-ra-no-av, forticlient-ra-no-fw, forticlient-ra-notinstalled, forticlient-ra-notlicensed, forticlient-ra-no-wf, forticlient-redir-portal, gbandwidth, groups,maxbandwidth, traffic-shaping`. Added fields `endpoint-allow-collect-sysinfo, endpoint-check, endpoint-redir-portal, endpoint-restrict-check, identity-based, traffic-shaper, traffic-shaper-reverse, session-ttl, wccp, match-vip`. New `config identity-based-policy` subcommand.
FortiOS v4.0 MR1	Removed fields `endpoint-allow-collect-sysinfo, endpoint-redir-portal, endpoint-restrict-check. Added field endpoint-profile`. Added `per-ip-shaper` and `fsae-server-for-ntlm` fields.

Related topics

- firewall policy, policy6
- firewall profile
- firewall schedule onetime firewall schedule recurring
- firewall service custom, firewall service group
- endpoint-control
- firewall interface-policy, firewall interface-policy6
- firewall sniff-interface-policy, firewall sniff-interface-policy6

profile

Use this command to configure protection profiles which can be applied to traffic by selecting the protection profile in one or more firewall policies, or by associating a protection profile with a firewall user group. The firewall policy will apply the subset of the protection profile that is relevant to the service or service group.

Syntax

```
config firewall profile
  edit <profile_str>
    set application-list-status {enable | disable}
    set application-list <name_string>
    set comment <comment_str>
    set dlp-sensor-table <name_string>
    set filepattable <index_int>
    set ftgd-wf-allow {all | <category_str>}
    set ftgd-wf-deny {all | <category_str>}
    set ftgd-wf-enable {all | <category_str>}
    set ftgd-wf-disable {all | <category_str>}
    set ftgd-wf-https-options {allow-ovrd error-allow rate-server-ip
       strict-blocking}
    set ftgd-wf-log {all | <category_str>}
    set ftgd-wf-options {allow-ovrd error-allow http-err-detail rate-image-
       urls rate-server-ip redir-block strict-blocking}
    set ftgd-wf-ovrd {all | <category_str>}
    set ftp {avmonitor avquery block clientcomfort no-content-summary
       oversize quarantine scan splice}
    set ftp-avdb {default | normal | extended}
    set ftpcomfortamount <size_int>
    set ftpcomfortinterval <seconds_int>
    set ftpoversizelimit <size_int>
    set http {activexfilter avmonitor avquery bannedword block block-
       invalid-url chunkedbypass clientcomfort cookiefilter fortiguard-wf
       javafilter no-content-summary oversize quarantine rangeblock scan
       strict-file urlfilter}
    set http-avdb {default | normal | extended}
    set httpcomfortamount <size_int>
    set httpcomfortinterval <seconds_int>
    set httpoversizelimit <size_int>
    set httppostaction {normal | comfort | block}
    set http-post-lang <charset1> [<charset2>... <charset5>]
    set http-retry-count <retry_int>
    set httpsoversizelimit <size_int>
    set https-retry-count <retry_int>
    set https {activexfilter allow-invalid-server-cert avmonitor avquery
       bannedword block block-invalid-url block-ssl-unknown-sess-id
       chunkedbypass clientcomfort cookiefilter fortiguard-wf javafilter
       log-invalid-server-cert no-content-summary oversize quarantine
       rangeblock scan strict-file urlfilter}
    set https-avdb {default | normal | extended}
    set https-deep-scan {enable | disable}
    set im {avmonitor avquery block oversize quarantine scan}
    set im-avdb {default | normal | extended}
```

```
set imap { avmonitor avquery bannedword block fragmail
   no-content-summary oversize quarantine scan spam-mail-log
   spamemailbwl spamfschksum spamfsip spamfssubmit spamfsurl
   spamhdrcheck spamipbwl spamraddrdns spamrbl}
set imapoversizelimit <size_int>
set imap-spamaction {pass | tag | discard}
set imap-spamtagtype{ subject header spaminfo}
set imap-spamtagmsg <text_string>
set imaps { allow-invalid-server-cert avmonitor avquery bannedword block
   fragmail log-invalid-server-cert no-content-summary oversize
   quarantine scan spam-mail-log spamemailbwl spamfschksum spamfsip
   spamfssubmit spamfsurl spamhdrcheck spamipbwl spamraddrdns spamrbl}
set imaps-avdb {default | normal | extended}
set imapsoversizelimit <size_int>
set imaps-spamaction {pass | tag | discard}
set imaps-spamtagtype{ subject header spaminfo}
set imap-spamtagmsg <text_string>
set imoversizelimit <size_int>
set ips-sensor <name_str>
set ips-sensor-status {enable | disable}
set mail-sig <signature_str>
set mailsig-status {enable | disable}
set nac-quar-infected {none quar-interface quar-src-ip}
set nac-quar-expiry {###d##h##m indefinite}
set nntp {avmonitor avquery block no-content-summary oversize quarantine
   scan spam-mail-log splice}
set nntp-avdb {default | normal | extended}
set nntpoversizelimit <limit_int>
set pop3 {avmonitor avquery bannedword block fragmail no-content-summary
   oversize quarantine scan spam-mail-log spamemailbwl spamfschksum
   spamfsip spamfssubmit spamfsurl spamhdrcheck spamipbwl spamraddrdns
   spamrbl}
set pop3-avdb {default | normal | extended}
set pop3oversizelimit <size_int>
set pop3-spamaction {pass | tag}
set pop3-spamtagmsg <message_str>
set pop3-spamtagtype {header | subject} {spaminfo | }
set pop3-spamaction {pass | tag}
set pop3s {allow-invalid-server-cert avmonitor avquery bannedword block
   fragmail log-invalid-server-cert no-content-summary oversize
   quarantine scan spam-mail-log spamemailbwl spamfschksum spamfsip
   spamfssubmit spamfsurl spamhdrcheck spamipbwl spamraddrdns spamrbl}
set pop3s-avdb {default | normal | extended}
set pop3soversizelimit <size_int>
set pop3s-spamaction {discard | pass | tag}
set pop3s-spamtagtype {header | subject} {spaminfo | }
set pop3s-spamtagmsg <message_str>
set replacemsg-group <name_str>
set safesearch {bing google yahoo}
set smtp {avmonitor avquery bannedword block fragmail no-content-summary
   oversize quarantine scan spam-mail-log spamemailbwl spamfsip
   spamfschksum spamfsurl spamhdrcheck spamhelodns spamipbwl
   spamraddrdns spamrbl splice}
set smtp-avdb {default | normal | extended}
```

```
    set smtps {allow-invalid-server-cert avmonitor avquery bannedword block
       fragmail log-invalid-server-cert no-content-summary oversize
       quarantine scan spam-mail-log spamemailbwl spamfsip spamfschksum
       spamfsurl spamhdrcheck spamhelodns spamipbwl spamraddrdns spamrbl
       splice}
    set smtps-avdb {default | normal | extended}
    set smtp-spam-localoverride {enable | disable}
    set smtpoversizelimit <size_int>
    set smtpsoversizelimit <size_int>
    set smtp-spamaction {discard | pass | tag}
    set smtp-spamhdrip {enable | disable}
    set smtp-spamtagmsg <message_str>
    set smtp-spamtagtype {header | subject} {spaminfo | }
    set smtps-spamaction {discard | pass | tag}
    set smtps-spamhdrip {enable | disable}
    set smtps-spamtagmsg <message_str>
    set smtps-spamtagmsg <message_str>
    set spambwordtable <index_int>
    set spamemaddrtable <index_int>
    set spamipbwltable <index_int>
    set spamiptrusttable <index_int>
    set spammheadertable <index_int>
    set spamrbltable <index_int>
    set spambwordthreshold <value_int>
    set webbwordtable <index_int>
    set webbwordthreshold <value_int>
    set webexmwordtable <index_int>
    set weburlfiltertable <index_int>
    config log
      set log-app-ctrl {enable | disable}
      set log-av-block {enable | disable}
      set log-av-oversize {enable | disable}
      set log-av-virus {enable | disable}
      set log-dlp {enable | disable}
      set log-ips {enable | disable}
      set log-spam {enable | disable}
      set log-web-content {enable | disable}
      set log-web-filter-activex {enable | disable}
      set log-web-filter-applet {enable | disable}
      set log-web-filter-cookie {enable | disable}
      set log-web-ftgd-err {enable | disable}
      set log-web-invalid-domain {enable | disable}
      set log-web-url {enable | disable}
    config app-recognition
    end
end
```

Variable	Description	Default
<profile_str>	Enter the name of this protection profile.	No default.
The following commands are the set options for edit <profile str>.		
application-list-status {enable | disable}	Enable or disable application control.	disable
application-list <name_string>	Set the application control list name. This option only appears after application-list-status is enable.	No default.
comment <comment_str>	Enter a comment about the protection profile. If the comment contains spaces or special characters, surround the comment with double quotes (“). Comments can be up to 64 characters long.	No default.
dlp-sensor-table <name_string>	Select a Data Leak Prevention sensor for the profile.	No default.
filepattable <index_int>	Enter the ID number of the file pattern list to be used with the protection profile. This option appears only on FortiGate-800 models and greater.	0
ftgd-wf-allow {all | <category_str>}	Enter all, or enter one or more category codes, representing FortiGuard Web Filtering web page categories or category groups that you want to allow. To view a list of available category codes with their descriptions, enter get, then locate entries for ftgd-wf-enable, such as g01 Potentially Liable, 1 Drug Abuse, and c06 Spam URL. Separate multiple codes with a space. To delete entries, use the unset command to delete the entire list. See also “webfilter fortiguard” on page 663.	All categories not specified as deny or monitor.
ftgd-wf-deny {all | <category_str>}	Enter all, or enter one or more category codes, representing FortiGuard Web Filtering web page categories or category groups that you want to block. To view a list of available category codes with their descriptions, enter get, then locate entries for ftgd-wf-enable, such as g01 Potentially Liable, 1 Drug Abuse, and c06 Spam URL. Separate multiple codes with a space. To delete entries, use the unset command to delete the entire list. See also “webfilter fortiguard” on page 663.	No default.
ftgd-wf-enable {all | <category_str>}	Enable categories for use in local ratings. You can enable categories, classes, and groups. To view a list of available category codes with their descriptions, enter get, then locate entries for ftgd-wf-enable, such as g01 Potentially Liable, 1 Drug Abuse, and c06 Spam URL. Separate multiple codes with a space. To delete entries, use the unset command to delete the entire list. See also “webfilter fortiguard” on page 663.	No default.
ftgd-wf-disable {all | <category_str>}	Disable categories for use in local ratings. You can disable categories, classes, and groups. To view a list of available category codes with their descriptions, enter get, then locate entries for ftgd-wf-enable, such as g01 Potentially Liable, 1 Drug Abuse, and c06 Spam URL. Separate multiple codes with a space. To delete entries, use the unset command to delete the entire list. See also “webfilter fortiguard” on page 663.	No default.

Variable	Description	Default
`ftgd-wf-https-options {allow-ovrd error-allow rate-server-ip strict-blocking}`	Select the options for FortiGuard Web Filtering category blocking. • `allow-ovrd`: Allow authenticated rating overrides. • `error-allow` to allow web pages with a rating error to pass through. • `rate-server-ip`: Rate both the URL and the IP address of the requested site, providing additional security against circumvention attempts. • `strict-blocking` to block any web pages if any classification or category matches the rating. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	`Null`
`ftgd-wf-log {all | <category_str>}`	Enter `all`, or enter one or more category codes, representing FortiGuard Web Filtering web page categories or category groups that you want to log. To view a list of available category codes with their descriptions, enter `get`, then locate entries for `ftgd-wf-enable`, such as `g01 Potentially Liable`, `1 Drug Abuse`, and `c06 Spam URL`. Separate multiple codes with a space. To delete entries, use the `unset` command to delete the entire list.	No default.
`ftgd-wf-options {allow-ovrd error-allow http-err-detail rate-image-urls rate-server-ip redir-block strict-blocking}`	Select options for FortiGuard web filtering, separating multiple options with a space. • `allow-ovrd`: Allow authenticated rating overrides. • `error-allow`: Allow web pages with a rating error to pass through. • `http-err-detail`: Display a replacement message for 4xx and 5xx HTTP errors. If error pages are allowed, malicious or objectionable sites could use these common error pages to circumvent web category blocking. This option does not apply to HTTPS. • `rate-image-urls`: Rate images by URL. Blocked images are replaced with blanks. This option does not apply to HTTPS. • `rate-server-ip`: Send both the URL and the IP address of the requested site for checking, providing additional security against attempts to bypass the FortiGuard system. • `redir-block`: Block HTTP redirects. Many web sites use HTTP redirects legitimately; however, in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect. • `strict-blocking`: Block any web pages if any classification or category matches the rating. This option does not apply to HTTPS. To remove an option from the list or add an option to the list, retype the list with the option removed or added. These options take effect only if FortiGuard web filtering is enabled for the protocol.	`Null`

Variable	Description	Default
`ftgd-wf-ovrd {all | <category_str>}`	Enter `all`, or enter one or more category codes, representing FortiGuard Web Filtering web page categories or category groups that you want to allow users to override. If filtering overrides are enabled for the protocol and a user requests a web page from a category that is blocked, the user is presented with an authentication challenge; if they successfully authenticate, they are permitted to bypass the filter and access the web page. User groups permitted to authenticate are defined in the firewall policy. For details, see "groups <group_name>" on page 135. To view a list of available category codes with their descriptions, enter `get`, then locate entries for `ftgd-wf-enable`, such as `g01 Potentially Liable`, `1 Drug Abuse`, and `c06 Spam URL`. Separate multiple codes with a space. To delete entries, use the `unset` command to delete the entire list.	No default.
`ftp {avmonitor avquery block clientcomfort no-content-summary oversize quarantine scan splice}`	Select actions, if any, the FortiGate unit will perform with FTP connections. `avmonitor`: Log detected viruses, but allow them through the firewall without modification. `avquery`: Use the FortiGuard AV query service. `block`: Deny files matching the file pattern selected by `filepattable`, even if the files do not contain viruses. `clientcomfort`: Apply client comforting and prevent client timeout. `no-content-summary`: Omit the content summary from the dashboard. `oversize`: Block files that are over the file size limit. `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or are connected to a FortiAnalyzer unit. `scan`: Scan files for viruses and worms. `splice`: Simultaneously scan a message and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	`splice`
`ftp-avdb {default | normal | extended}`	Select the antivirus database to use for FTP: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`
`ftpcomfortamount <size_int>`	Enter the number of bytes client comforting sends each interval to show that an FTP download is progressing. The interval time is set using `ftpcomfortinterval`.	1
`ftpcomfortinterval <seconds_int>`	Enter the time in seconds before client comforting starts after an FTP download has begun. It is also the interval between subsequent client comforting sends. The amount of data sent each interval is set using `ftpcomfortamount`.	10
`ftpoversizelimit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `ftpoversizelimit`, the file is passed or blocked, depending on whether `ftp` contains the `oversize` option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	10

Variable	Description	Default

`http`
`{activexfilter`
`avmonitor`
`avquery`
`bannedword`
`block`
`block-invalid-url`
`chunkedbypass`
`clientcomfort`
`cookiefilter`
`fortiguard-wf`
`javafilter`
`no-content-summary`
`oversize`
`quarantine`
`rangeblock`
`scan`
`strict-file`
`urlfilter}`
	Select actions, if any, the FortiGate unit will perform with HTTP connections.
	`activexfilter`: Block ActiveX plugins.
	`avmonitor`: Log detected viruses, but allow them through the firewall without modification.
	`avquery`: Use the FortiGuard Antivirus service for virus detection using MD5 checksums. This feature is disabled by default.
	`bannedword`: Block web pages containing content in the banned word list.
	`block`: Deny files matching the file pattern selected by `filepattable`, even if the files do not contain viruses.
	`block-invalid-url:` Block sessions containing an invalid domain name.
	`chunkedbypass`: Allow web sites that use chunked encoding for HTTP to bypass the firewall. Chunked encoding means the HTTP message body is altered to allow it to be transferred in a series of chunks. Use of this feature is a risk. Malicious content could enter the network if web content is allowed to bypass the firewall.
	`clientcomfort`: Apply client comforting and prevent client timeout.
	`cookiefilter`: Block cookies.
	`fortiguard-wf`: Use FortiGuard Web Filtering.
	`javafilter`: Block Java applets.
	`no-content-summary`: Omit content information from the dashboard.
	`oversize`: Block files that are over the file size limit.
	`quarantine`: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or are connected to a FortiAnalyzer unit.
	`rangeblock`: Block downloading parts of a file that have already been partially downloaded. Enabling this option prevents the unintentional download of virus files hidden in fragmented files. Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions. Enabling this option may break certain applications that use the Range Header in the HTTP protocol, such as YUM, a Linux update manager.
	`scan`: Scan files for viruses and worms.
	`strict-file` to perform stricter checking for blocked files as specified by antivirus file patterns. This more thorough checking can effectively block some web sites with elaborate scripting using `.exe` or `.dll` files if those patterns are blocked.
	`urlfilter`: Use the URL filter list.
	Separate multiple options with a space.To remove an option from the list or add an option to the list, retype the list with the option removed or added.
		No default.

Variable	Description	Default
`http-avdb {default | normal | extended}`	Select the antivirus database to use for HTTP: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment. The extended antivirus data is available on newer FortiGate models with more than one partition, for example: • FortiGate-50B and FortiWiFi-50B • FortiGate-60B and FortiWiFi-60B • FortiGate-310B • FortiGate-1000A and FortiGate-1000AFA2 • FortiGate-1000A-LENC • FortiGate-3016B, FortiGate-3600A, and FortiGate-3810A • FortiGate-5005FA2 and FortiGate-5001A	`default`
`httpcomfortamount <size_int>`	Enter the number of bytes client comforting sends each interval to show an HTTP download is progressing. The interval time is set using `httpcomfortinterval`.	1
`httpcomfortinterval <seconds_int>`	Enter the time in seconds before client comforting starts after an HTTP download has begun. It is also the interval between subsequent client comforting sends. The amount of data sent each interval is set using `httpcomfortamount`.	10
`httpoversizelimit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `httpoversizelimit`, the file is passed or blocked, depending on whether `oversize` is set in the profile `http` command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	10
`httpsoversizelimit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `httpsoversizelimit`, the file is passed or blocked, depending on whether `oversize` is set in the profile `https` command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	10
`httppostaction {normal | comfort | block}`	Select the action to take with HTTP POST traffic: `normal`: Do not affect HTTP POST traffic. `comfort`: Use the `httpcomfortamount` amount and `httpcomfortinterval` settings to send "comfort" bytes to the server in case the client connection is too slow. Select this option to prevent a server timeout when scanning or other filtering tool is turned on. `block`: Block HTTP POST requests. When the post request is blocked the FortiGate unit sends the `http-post-block` replacement message to the user's web browser.	`normal`

Variable	Description	Default
`http-post-lang <charset1> [<charset2>... <charset5>]`	The FortiGate unit converts HTTP, HTTPS, and email content to the UTF-8 character set before applying spam filtering banned word checking, web filtering and DLP content scanning as specified in the protection profile. For email messages, while parsing the MIME content, the FortiGate unit converts the content to UTF-8 encoding according to the email message charset field before applying Spam filtering banned word checking and DLP scanning. For HTTP get pages, the FortiGate unit converts the content to UTF-8 encoding according to the character set specified for the page before applying web content filtering and DLP scanning. For HTTP post pages, because character sets are not always accurately indicated in HTTP posts, you can use the `http-post-lang` option to specify up to five character set encodings. The FortiGate unit performs a forced conversion of HTTP post pages to UTF-8 for each specified character set. After each conversion the FortiGate unit applies web content filtering and DLP scanning to the content of the converted page. **Caution:** Specifying multiple character sets reduces web filtering and DLP performance. To view the list of available character sets, enter `set http-post-lang ?` from within the edit shell for the protection profile. Separate multiple character set names with a space. You can add up to 5 character set names.	0
`http-retry-count <retry_int>`	Enter the number of times to retry establishing an HTTP connection when the connection fails on the first try. The range is 0 to 100. This allows the web server proxy to repeat the connection attempt on behalf of the browser if the server refuses the connection the first time. This works well and reduces the number of hang-ups or page not found errors for busy web servers. Entering zero (`0`) effectively disables this feature.	0
`httppostaction {block comfort normal}`	Select the action to take against HTTP uploads. `Block:` Ban HTTP POST operations. `Comfort:` Use the comfort amount and interval settings to send “comfort” bytes to the server in case the client connection is too slow. This is to prevent a timeout when scanning or other filtering tool is turned on. `Normal:` Allow the traffic to pass, subject to the results of FortiGate firewall screening.	`normal`
`https-retry-count <retry_int>`	Enter the number of times to retry establishing an HTTPs connection when the connection fails on the first try. The range is 0 to 100. This allows the web server proxy to repeat the connection attempt on behalf of the browser if the server refuses the connection the first time. This works well and reduces the number of hang-ups or page not found errors for busy web servers. Entering zero (`0`) effectively disables this feature.	0

Variable	Description	Default

`https`
`{activexfilter`
`allow-invalid-server-cert`
`avmonitor`
`avquery`
`bannedword`
`block`
`block-invalid-url`
`block-ssl-unknown-sess-id`
`chunkedbypass`
`clientcomfort`
`cookiefilter`
`fortiguard-wf`
`javafilter`
`log-invalid-server-cert`
`no-content-summary`
`oversize`
`quarantine`
`rangeblock`
`scan`
`strict-file`
`urlfilter}`
	Select actions, if any, the FortiGate unit will perform with HTTPS connections.
	• `activexfilter`: Block ActiveX plugins.
	• `allow-invalid-server-cert:` Allow SSL sessions whose server certificate validation failed.
	• `avmonitor`: Log detected viruses, but allow them through the firewall without modification.
	• `avquery`: Use the FortiGuard Antivirus service for virus detection using MD5 checksums. This feature is disabled by default.
	• `bannedword`: Block web pages containing content in the banned word list.
	• `block`: Deny files matching the file pattern selected by `filepattable`, even if the files do not contain viruses.
	• `block-invalid-url`: Block web sites whose SSL certificate's CN field does not contain a valid domain name. FortiGate units always validate the CN field, regardless of whether this option is enabled. However, if this option is disabled, although validation failure does not cause the FortiGate unit to block the request, it changes the behavior of FortiGuard Web Filtering.
	If the request is made directly to the web server, rather than a web server proxy, the FortiGate unit queries for FortiGuard Web Filtering category or class ratings using the IP address only, not the domain name.
	If the request is to a web server proxy, the real IP address of the web server is not known, and so rating queries by either or both the IP address and the domain name is not reliable. In this case, the FortiGate unit does not perform FortiGuard Web Filtering.
	• `block-ssl-unknown-sess-id`: Enable blocking of SSL sessions whose ID has not been previously filtered. If HTTPS web filtering is enabled, session IDs may be regenerated by the server, which in turn will reject some HTTPS sessions based on the 'unknown session ID' test. This option allows for unknown (encrypted SSL data) session IDs by default.
	• `chunkedbypass`: Allow web sites that use chunked encoding for HTTP to bypass the firewall. Chunked encoding means the HTTP message body is altered to allow it to be transferred in a series of chunks. Use of this feature is a risk. Malicious content could enter the network if web content is allowed to bypass the firewall.
	• `clientcomfort`: Apply client comforting and prevent client timeout.
	• `cookiefilter`: Block cookies.
		No default.

Variable	Description	Default
	• `fortiguard-wf`: Enable FortiGuard Web Filtering. • `javafilter`: Block Java applets. • `log-invalid-server-cert`: Log SSL sessions whose server certificate validation failed. • `no-content-summary`: Omit content information from the dashboard. • `oversize`: Block files that are over the file size limit. • `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or are connected to a FortiAnalyzer unit. • `rangeblock`: Block downloading parts of a file that have already been partially downloaded. Enabling this option prevents the unintentional download of virus files hidden in fragmented files. Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions. Enabling this option may break certain applications that use the Range Header in the HTTP protocol, such as YUM, a Linux update manager. • `scan`: Scan files for viruses and worms. • `strict-file` to perform stricter checking for blocked files as specified by antivirus file patterns. This more thorough checking can effectively block some web sites with elaborate scripting using `.exe` or `.dll` files if those patterns are blocked. • Enter `urlfilter` to enable the URL filter list. Separate multiple options with a space.To remove an option from the list or add an option to the list, retype the list with the option removed or added.	
`https-avdb {default | normal | extended}`	Select the antivirus database to use for HTTPS: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`
`https-deep-scan {enable | disable}`	Select to decrypt HTTPS traffic and perform additional scanning of the content of the HTTPS traffic. Select this option if you want to apply all applicable protection profile options to HTTPS traffic. Using this option requires adding HTTPS server certificates to the FortiGate unit so that HTTPS traffic can be unencrypted.	`disable`
`httpscomfortinterval <seconds_int>`	Enter the time in seconds before client comforting starts after an HTTPs download has begun. It is also the interval between subsequent client comforting sends. The amount of data sent each interval is set using `httspcomfortamount`.	10
`httpscomfortamount <size_int>`	Enter the number of bytes client comforting sends each interval to show an HTTPs download is progressing. The interval time is set using `httpscomfortinterval`.	1

Variable	Description	Default
`im {avmonitor avquery block oversize quarantine scan}`	Select actions, if any, the FortiGate unit will perform with instant message (IM) connections. • `avmonitor`: Log detected viruses, but allow them through the firewall without modification. • `avquery`: Use the FortiGuard Antivirus service for virus detection using MD5 checksums. • `oversize`: Block files that are over the file size limit. • `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or are connected to a FortiAnalyzer unit. • `scan`: Scan files for viruses and worms.	No default.
`im-avdb {default | normal | extended}`	Select the antivirus database to use for IM: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`

Variable	Description	Default
imap { avmonitor avquery bannedword block fragmail no-content-summary oversize quarantine scan spam-mail-log spamemailbwl spamfschksum spamfsip spamfssubmit spamfsurl spamhdrcheck spamipbwl spamraddrdns spamrbl}	Select actions, if any, the FortiGate unit will perform with IMAP connections. • avmonitor: Log detected viruses, but allow them through the firewall without modification. • avquery: Use the FortiGuard Antivirus service for virus detection using MD5 checksums. • bannedword: Block email containing content on the banned word list. • block: Deny files matching the file pattern selected by filepattable, even if the files do not contain viruses. • fragmail: Allow fragmented email. Fragmented email cannot be scanned for viruses. • no-content-summary: Omit content information from the dashboard.nto email, ftp, and http categories. • oversize: Block files that are over the file size limit. • quarantine to enable quarantining files that contain viruses. This feature is available for FortiGate units that contain a hard disk. • scan: Scan files for viruses and worms. • spam-mail-log to include spam in mail log. • spamemailbwlto enable filtering based on the email address list. • spamfschksum to enable the FortiGuard Antispam email message checksum spam check. • spamfsip to enable the FortiGuard Antispam filtering IP address blacklist. • spamfssubmit to add a link to the message body to allow users to report messages incorrectly marked as spam. If an email message is not spam, simply click the link in the message to inform FortiGuard of the false positive. • spamfsurl to enable the FortiGuard Antispam filtering URL blacklist. • spamhdrcheck to enable email mime header check. • spamipbwl to enable filtering based on the email ip address. • spamaddrdns to enable filtering based on the return email DNS check. • spamrbl to enable checking traffic against configured DNS-based Blackhole List (DNSBL) and Open Relay Database List (ORDBL) servers. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	spamfssubmit
imap-avdb {default | normal | extended}	Select the antivirus database to use for IMAP: default: Use the database selected in antivirus settings. normal: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. extended: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	default
imap-spamaction {pass | tag | discard}	Select action on spam. • pass: Allow spam email to pass. • tag: Tag spam email with configured text in subject or header. • discard: Do not pass email identified as spam.	tag

Variable	Description	Default
imap-spamtagtype{ subject header spaminfo}	Choose tag subject or header for spam email. • subject: Prepend text to spam email subject. • header: Append a user defined mime header to spam email. • spaminfo: Append spam info to spam email header.	subject spaminfo
imap-spamtagmsg <text_string>	Add subject text or header to spam email.	Spam
imaps { allow-invalid-server-cert avmonitor avquery bannedword block fragmail log-invalid-server-cert no-content-summary oversize quarantine scan spam-mail-log spamemailbwl spamfschksum spamfsip spamfssubmit spamfsurl spamhdrcheck spamipbwl spamraddrdns spamrbl}	Select actions, if any, the FortiGate unit will perform with IMAP connections. • allow-invalid-server-cert: Allow SSL sessions whose server certificate validation failed. • avmonitor: Log detected viruses, but allow them through the firewall without modification. • avquery: Use the FortiGuard Antivirus service for virus detection using MD5 checksums. • bannedword: Block email containing content on the banned word list. • block: Deny files matching the file pattern selected by filepattable, even if the files do not contain viruses. • fragmail: Allow fragmented email. Fragmented email cannot be scanned for viruses. • log-invalid-server-cert: Log SSL sessions whose server certificate validation failed. • no-content-summary: Omit content information from the dashboard.nto email, ftp, and http categories. • oversize: Block files that are over the file size limit. • quarantine to enable quarantining files that contain viruses. This feature is available for FortiGate units that contain a hard disk. • scan: Scan files for viruses and worms. • spam-mail-log to include spam in mail log. • spamemailbwlto enable filtering based on the email address list. • spamfschksum to enable the FortiGuard Antispam email message checksum spam check. • spamfsip to enable the FortiGuard Antispam filtering IP address blacklist. • spamfssubmit to add a link to the message body to allow users to report messages incorrectly marked as spam. If an email message is not spam, simply click the link in the message to inform FortiGuard of the false positive. • spamfsurl to enable the FortiGuard Antispam filtering URL blacklist. • spamhdrcheck to enable email mime header check. • spamipbwl to enable filtering based on the email ip address. • spamaddrdns to enable filtering based on the return email DNS check. • spamrbl to enable checking traffic against configured DNS-based Blackhole List (DNSBL) and Open Relay Database List (ORDBL) servers. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	spamfssubmit

Variable	Description	Default
`imaps-avdb {default | normal | extended}`	Select the antivirus database to use for IMAPS: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`
`imaps-spamaction {pass | tag | discard}`	Select action on spam. • `pass`: Allow spam email to pass. • `tag`: Tag spam email with configured text in subject or header. • `discard`: Do not pass email identified as spam.	`tag`
`imaps-spamtagtype{ subject header spaminfo}`	Choose tag subject or header for spam email. • `subject:` Prepend text to spam email subject. • `header:` Append a user defined mime header to spam email. • `spaminfo:` Append spam info to spam email header.	`subject spaminfo`
`imap-spamtagmsg <text_string>`	Add subject text or header to spam email.	`Spam`
`imapoversizelimit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `imapoversizelimit`, the file is passed or blocked, depending on whether `oversize` is set in the profile `imap` command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. **Note:** For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the configured oversize threshold.	`10`
`imapsoversizelimit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `imapsoversizelimit`, the file is passed or blocked, depending on whether `oversize` is set in the profile `imap` command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. **Note:** For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the configured oversize threshold.	`10`
`imoversizelimit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `imoversizelimit`, the file is passed or blocked, depending on whether `oversize` is set in the profile `im` command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`
`ips-sensor <name_str>`	Enter the name of an IPS sensor (set of signatures).	No default.

Variable	Description	Default
`ips-sensor-status {enable | disable}`	Select to use an IPS sensor. If enabled, also configure `ips-sensor`. This option does not select denial of service (DoS) sensors. For details on configuring DoS sensors, see "ips DoS" on page 220.	`disable`
`mail-sig <signature_str>`	Enter a signature to add to outgoing email. If the signature contains spaces, surround it with single or double quotes (‘ or "). This option is applied only if `mailsig-status` is `enable`.	No default.
`mailsig-status {enable | disable}`	Select to add a signature to outgoing email. Also configure `mail-sig`.	`disable`
`nac-quar-infected {none quar-interface quar-src-ip}`	Select to quarantine infected hosts to banned user list. • `none`: No action is taken. • `quar-interface:` Quarantine all traffic on infected interface. • `quar-src-ip:` Quarantine all traffic from source IP.	`none`
`nac-quar-expiry {###d##h##m indefinite}`	Set the duration of quarantine. The minimum is `0d0h5m` and the maximum is `indefinite`.	`indefinite`
`nntp {avmonitor avquery block no-content-summary oversize quarantine scan spam-mail-log splice}`	Select actions, if any, the FortiGate unit will perform with NNTP connections. • `archive-full`: Content archive both metadata and the mail itself. • `archive-summary`: Content archive metadata. • `avmonitor`: Log detected viruses, but allow them through the firewall without modification. • `avquery`: Use the FortiGuard Antivirus query service. • `block`: Deny files matching the file pattern selected by `filepattable`, even if the files do not contain viruses. • `no-content-summary`: Omit content information from the dashboard. • `oversize`: Block files that are over the file size limit. • `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or are connected to a FortiAnalyzer unit. • `scan`: Scan files for viruses and worms. • `spam-mail-log`: Include spam in the mail log. • Streaming mode (also called `splice`) is enabled by default when `scan` is enabled. Streaming mode has the FortiGate unit simultaneously scan a message and send it to the recipient. If the FortiGate unit detects a virus, it terminates the server connection and returns an error message to the recipient, listing the virus name and infected file name. When streaming mode is disabled for NNTP, infected attachments are removed and the message is sent (without the attachment) to the recipient. Throughput is higher when streaming mode is enabled. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	No default.
`nntp-avdb {default | normal | extended}`	Select the antivirus database to use for NNTP: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`

Variable	Description	Default
`nntpoversizelimit <limit_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `ntpoversizelimit`, the file is passed or blocked, depending on whether `oversize` is set in the profile `nntp` command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	10
`pop3 {avmonitor avquery bannedword block fragmail no-content-summary oversize quarantine scan spam-mail-log spamemailbwl spamfschksum spamfsip spamfssubmit spamfsurl spamhdrcheck spamipbwl spamraddrdns spamrbl}`	Select actions, if any, the FortiGate unit will perform with POP3 connections. • `avmonitor`: Log detected viruses, but allow them through the firewall without modification. • `avquery`: Use the FortiGuard Antivirus query service. • `bannedword`: Block email containing content in the banned word list. • `block`: Deny files matching the file pattern selected by `filepattable`, even if the files do not contain viruses. • `fragmail`: Allow fragmented email. Fragmented email cannot be scanned for viruses. • `no-content-summary`: Omit content information from the dashboard.nto email, FTP, and HTTP categories. • `oversize`: Block files that are over the file size limit. • `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or a connection to a FortiAnalyzer unit. • `scan`: Scan files for viruses and worms. • `spam-mail-log`: Include spam in the email log. • `spamemailbwl`: Block email containing addresses in the email address list. • `spamfschksum`: Use FortiGuard Antispam email message checksum spam checking. • `spamfsip`: Use the FortiGuard Antispam IP address blacklist. • `spamfssubmit`: Add a link to the message body to allow users to report messages incorrectly marked as spam. If an email message is not spam, click the link in the message to inform FortiGuard of the false positive. • `spamfsurl`: Use the FortiGuard Antispam URL blacklist. • `spamhdrcheck`: Filter email using the MIME header list. • `spamipbwl`: Filter email using the email IP address. • `spamaddrdns`: Filter email using the return email DNS check. • `spamrbl`: Filter email using the configured DNS-based Blackhole List (DNSBL) and Open Relay Database List (ORDBL) servers. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	`spamfssubmit`
`pop3-avdb {default | normal | extended}`	Select the antivirus database to use for POP3: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`

Variable	Description	Default
pop3oversizelimit <size_int>	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the pop3oversizelimit, the file is passed or blocked, depending on whether oversize is set in the profile pop3 command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. **Note:** For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the configured oversize threshold.	10
pop3-spamaction {pass | tag}	Select the action to perform on POP3 email that is detected as spam. • pass: Disable spam filtering for POP3 traffic. • tag: Tag spam email with text configured using the pop3-spamtagmsg field and the location set using the pop3-spamtagtype field.	tag
pop3-spamtagmsg <message_str>	Enter a word or phrase (tag) to affix to email identified as spam. When typing a tag, use the same language as the FortiGate unit's current administrator language setting. Tag text using other encodings may not be accepted. For example, when entering a spam tag that uses Japanese characters, first verify that the administrator language setting is Japanese; the FortiGate unit will not accept a spam tag written in Japanese characters while the administrator language setting is English. For details on changing the language setting, see "system global" on page 423. **Note:** To correctly enter the tag, your SSH or telnet client must also support your language's encoding. Alternatively, you can use the web-based manager's CLI widget to enter the tag. Tags must not exceed 64 bytes. The number of characters constituting 64 bytes of data varies by text encoding, which may vary by the FortiGate administrator language setting. Tags containing space characters, such as multiple words or phrases, must be surrounded by quote characters (')to be accepted by the CLI.	Spam
pop3-spamtagtype {header | subject} {spaminfo | }	Select to affix the tag to either the MIME header or the subject line, and whether or not to append spam information to the spam header, when an email is detected as spam. Also configure pop3-spamtagmsg. If you select to affix the tag to the subject line, the FortiGate unit will convert the entire subject line, including tag, to UTF-8 by default. This improves display for some email clients that cannot properly display subject lines that use more than one encoding. For details on disabling conversion of subject line to UTF-8, see "system settings" on page 517.	subject spaminfo

Variable	Description	Default
`pop3s {allow-invalid-server-cert avmonitor avquery bannedword block fragmail log-invalid-server-cert no-content-summary oversize quarantine scan spam-mail-log spamemailbwl spamfschksum spamfsip spamfssubmit spamfsurl spamhdrcheck spamipbwl spamraddrdns spamrbl}`	Select actions, if any, the FortiGate unit will perform with POP3 connections. • `allow-invalid-server-cert:` Allow SSL sessions whose server certificate validation failed. • `avmonitor`: Log detected viruses, but allow them through the firewall without modification. • `avquery`: Use the FortiGuard Antivirus query service. • `bannedword`: Block email containing content in the banned word list. • `block`: Deny files matching the file pattern selected by `filepattable`, even if the files do not contain viruses. • `fragmail`: Allow fragmented email. Fragmented email cannot be scanned for viruses. • `log-invalid-server-cert:` Log SSL sessions whose server certificate validation failed. • `no-content-summary`: Omit content information from the dashboard.nto email, FTP, and HTTP categories. • `oversize`: Block files that are over the file size limit. • `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or a connection to a FortiAnalyzer unit. • `scan`: Scan files for viruses and worms. • `spam-mail-log`: Include spam in the email log. • `spamemailbwl`: Block email containing addresses in the email address list. • `spamfschksum`: Use FortiGuard Antispam email message checksum spam checking. • `spamfsip`: Use the FortiGuard Antispam IP address blacklist. • `spamfssubmit`: Add a link to the message body to allow users to report messages incorrectly marked as spam. If an email message is not spam, click the link in the message to inform FortiGuard of the false positive. • `spamfsurl`: Use the FortiGuard Antispam URL blacklist. • `spamhdrcheck`: Filter email using the MIME header list. • `spamipbwl`: Filter email using the email IP address. • `spamaddrdns`: Filter email using the return email DNS check. • `spamrbl`: Filter email using the configured DNS-based Blackhole List (DNSBL) and Open Relay Database List (ORDBL) servers. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	`spamfssubmit`
`pop3s-avdb {default | normal | extended}`	Select the antivirus database to use for POP3S: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`

Variable	Description	Default
pop3soversizelimit <size_int>	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the pop3soversizelimit, the file is passed or blocked, depending on whether oversize is set in the profile pop3s command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. **Note:** For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the configured oversize threshold.	10
pop3s-spamaction {discard | pass | tag}	Select the action that this profile uses for filtered POP3s email. Tagging appends custom text to the subject or header of email identified as spam. When scan or streaming mode (also called splice) is selected, the FortiGate unit can only discard spam email. Discard immediately drops the connection. Without streaming mode or scanning enabled, chose to discard, pass, or tag POP3s spam. In the US Domestic distribution, streaming mode is permanently enabled for POP3s, and the tag option is not available. • discard: Do not pass email identified as spam. • pass: Disable spam filtering for POP3s traffic. • tag: Tag spam email with text configured using the pop3s-spamtagmsg field and the location set using the pop3s-spamtagtype field.	tag
pop3s-spamtagtype {header | subject} {spaminfo | }	Select to affix the tag to either the MIME header or the subject line, and whether or not to append spam information to the spam header, when an email is detected as spam. Also configure pop3s-spamtagmsg. If you select to affix the tag to the subject line, the FortiGate unit will convert the entire subject line, including tag, to UTF-8 by default. This improves display for some email clients that cannot properly display subject lines that use more than one encoding. For details on disabling conversion of subject line to UTF-8, see "system settings" on page 517.	subject spaminfo
pop3s-spamtagmsg <message_str>	Enter a word or phrase (tag) to affix to email identified as spam. When typing a tag, use the same language as the FortiGate unit's current administrator language setting. Tag text using other encodings may not be accepted. For example, when entering a spam tag that uses Japanese characters, first verify that the administrator language setting is Japanese; the FortiGate unit will not accept a spam tag written in Japanese characters while the administrator language setting is English. For details on changing the language setting, see "system global" on page 423. **Note:** To correctly enter the tag, your SSH or telnet client must also support your language's encoding. Alternatively, you can use the web-based manager's CLI widget to enter the tag. Tags must not exceed 64 bytes. The number of characters constituting 64 bytes of data varies by text encoding, which may vary by the FortiGate administrator language setting. Tags containing space characters, such as multiple words or phrases, must be surrounded by quote characters (') to be accepted by the CLI.	Spam
replacemsg-group <name_str>	Enter the name of the replacement message group to be used with this protection profile. In FortiOS, you can select only the default group.	default

Variable	Description	Default
`safesearch {bing google yahoo}`	Enforce the strictest level the safe search feature of the Google, Yahoo!, and Bing search engines. This feature works by manipulating search URL requests to add code used by the safe search features of the search engines. Enforcing safe searching provides additional protection in environments such as schools or other environments that use web filtering to block sites with inappropriate content. Web Filtering alone may not block offensive content that appears search results. This offensive content could include offensive text in search results or offensive images in image search results. Enter one or more options to enable one or more safe searches. • `bing`: Enforce the strict level of safe search protection for Bing searches by adding *adlt=strict* to search URL requests. • `google`: enforce the strict filtering level of safe search protection for Google searches by adding *&safe=on* to search URL requests. Strict filtering filters both explicit text and explicit images. • `yahoo`: Enforce filtering out adult web, video, and image search results from Yahoo! searches by adding *&vm=r* to search URL requests.	

Variable	Description	Default
`smtp {avmonitor avquery bannedword block fragmail no-content-summary oversize quarantine scan spam-mail-log spamemailbwl spamfsip spamfschksum spamfsurl spamhdrcheck spamhelodns spamipbwl spamraddrdns spamrbl splice}`	Select actions, if any, the FortiGate unit will perform with SMTP connections. • `avmonitor`: Log detected viruses, but allow them through the firewall without modification. • `avquery`: Use the FortiGuard AV query service. • `bannedword`: Block email containing content in the banned word list. • `block`: Deny files matching the file pattern selected by `filepattable`, even if the files do not contain viruses. • `fragmail`: Allow fragmented email. Fragmented email cannot be scanned for viruses. • `no-content-summary`: Omit content information from the dashboard. • `oversize`: Block files that are over the file size limit. • `quarantine`: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or a connection to a FortiAnalyzer unit. • `scan`: Scan files for viruses and worms. • `spam-mail-log`: Include spam in the email log. • `spamemailbwl`: Filter email using the email address list. • `spamfsip`: Use the FortiGuard Antispam filtering IP address blacklist. • `spamfschksum`: Use FortiGuard Antispam email message checksum spam checking. • `spamfssubmit`: Add a link to the message body allowing users to report messages incorrectly marked as spam. If an email message is not spam, click the link in the message to report the false positive. • `spamfsurl`: Use the FortiGuard Antispam filtering URL blacklist. • `spamhdrcheck`: Filter email using the MIME header list. • `spamhelodns`: Filter email using an HELO/EHLO DNS check. • `spamipbwl`: Filter email using the source IP or subnet address. • `spamaddrdns`: Filter email using a return email DNS check. • `spamrbl`: Filter email using configured DNS-based Blackhole List (DNSBL) and Open Relay Database List (ORDBL) servers. • `splice`: Simultaneously scan a message and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection, and returns an error message to the sender, listing the virus and infected file name. `splice` is selected when `scan` is selected. With streaming mode enabled, select either Spam Action (Tagged or Discard) for SMTP spam. When streaming mode is disabled for SMTP, infected attachments are removed and the email is forwarded (without the attachment) to the SMTP server for delivery to the recipient. Throughput is higher when streaming mode is enabled. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	`spamfssubmit splice`

Variable	Description	Default
`smtp-avdb {default | normal | extended}`	Select the antivirus database to use for SMTP: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`
`smtp-spam-localoverride {enable | disable}`	Select to override SMTP remote check, which includes IP RBL check, IP FortiGuard antispam check, and HELO DNS check, with the locally defined black/white antispam list.	`disable`
`smtpoversizelimit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `smtpoversizelimit`, the file is passed or blocked, depending on whether `oversize` is set in the profile `smtp` command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. **Note:** For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the configured oversize threshold.	10
`smtpsoversizelimit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `smtpsoversizelimit`, the file is passed or blocked, depending on whether `oversize` is set in the profile `smtps` command. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. **Note:** For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes smaller than the configured oversize threshold.	10
`smtp-spamaction {discard | pass | tag}`	Select the action that this profile uses for filtered SMTP email. Tagging appends custom text to the subject or header of email identified as spam. When `scan` or streaming mode (also called `splice`) is selected, the FortiGate unit can only discard spam email. Discard immediately drops the connection. Without streaming mode or scanning enabled, chose to discard, pass, or tag SMTP spam. In the US Domestic distribution, streaming mode is permanently enabled for SMTP, and the tag option is not available. • `discard`: Do not pass email identified as spam. • `pass`: Disable spam filtering for SMTP traffic. • `tag`: Tag spam email with text configured using the `smtp-spamtagmsg` field and the location set using the `smtp-spamtagtype` field.	`discard`
`smtp-spamhdrip {enable | disable}`	Select to check header IP addresses for `spamfsip, spamrbl, and spamipbwl` filters.	`disable`

Variable	Description	Default
`smtp-spamtagmsg <message_str>`	Enter a word or phrase (tag) to affix to email identified as spam. When typing a tag, use the same language as the FortiGate unit's current administrator language setting. Tag text using other encodings may not be accepted. For example, when entering a spam tag that uses Japanese characters, first verify that the administrator language setting is Japanese; the FortiGate unit will not accept a spam tag written in Japanese characters while the administrator language setting is English. For details on changing the language setting, see "system global" on page 423. **Note:** To correctly enter the tag, your SSH or telnet client must also support your language's encoding. Alternatively, you can use the web-based manager's CLI widget to enter the tag. Tags must not exceed 64 bytes. The number of characters constituting 64 bytes of data varies by text encoding, which may vary by the FortiGate administrator language setting. Tags containing space characters, such as multiple words or phrases, must be surrounded by quote characters (') to be accepted by the CLI.	`Spam`
`smtp-spamtagtype {header | subject} {spaminfo | }`	Select to affix the tag to either the MIME header or the subject line, and whether or not to append spam information to the spam header, when an email is detected as spam. Also configure `smtp-spamtagmsg`. If you select to affix the tag to the subject line, the FortiGate unit will convert the entire subject line, including tag, to UTF-8 by default. This improves display for some email clients that cannot properly display subject lines that use more than one encoding. For details on disabling conversion of subject line to UTF-8, see "system settings" on page 517.	`subject spaminfo`

Variable	Description	Default
smtps {allow-invalid-server-cert avmonitor avquery bannedword block fragmail log-invalid-server-cert no-content-summary oversize quarantine scan spam-mail-log spamemailbwl spamfsip spamfschksum spamfsurl spamhdrcheck spamhelodns spamipbwl spamraddrdns spamrbl splice}	Select actions, if any, the FortiGate unit will perform with SMTP connections. • allow-invalid-server-cert: Allow SSL sessions whose server certificate validation failed • avmonitor: Log detected viruses, but allow them through the firewall without modification. • avquery: Use the FortiGuard AV query service. • bannedword: Block email containing content in the banned word list. • block: Deny files matching the file pattern selected by filepattable, even if the files do not contain viruses. • fragmail: Allow fragmented email. Fragmented email cannot be scanned for viruses. • log-invalid-server-cert: Log SSL sessions whose server certificate validation failed. • no-content-summary: Omit content information from the dashboard. • oversize: Block files that are over the file size limit. • quarantine: Quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or a connection to a FortiAnalyzer unit. • scan: Scan files for viruses and worms. • spam-mail-log: Include spam in the email log. • spamemailbwl: Filter email using the email address list. • spamfsip: Use the FortiGuard Antispam filtering IP address blacklist. • spamfschksum: Use FortiGuard Antispam email message checksum spam checking. • spamfssubmit: Add a link to the message body allowing users to report messages incorrectly marked as spam. If an email message is not spam, click the link in the message to report the false positive. • spamfsurl: Use the FortiGuard Antispam filtering URL blacklist. • spamhdrcheck: Filter email using the MIME header list. • spamhelodns: Filter email using an HELO/EHLO DNS check.spamipbwl: Filter email using the source IP or subnet address. • spamaddrdns: Filter email using a return email DNS check. • spamrbl: Filter email using configured DNS-based Blackhole List (DNSBL) and Open Relay Database List (ORDBL) servers. • splice: Simultaneously scan a message and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection, and returns an error message to the sender, listing the virus and infected file name. splice is selected when scan is selected. With streaming mode enabled, select either Spam Action (Tagged or Discard) for SMTP spam. When streaming mode is disabled for SMTP, infected attachments are removed and the email is forwarded (without the attachment) to the SMTP server for delivery to the recipient. Throughput is higher when streaming mode is enabled. Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.	spamfssubmit splice

Variable	Description	Default
`smtps-avdb {default | normal | extended}`	Select the antivirus database to use for SMTPS: `default`: Use the database selected in antivirus settings. `normal`: Use the regular virus database. The FortiGuard virus database includes "In the Wild" viruses and most commonly seen viruses on the network. This database is sufficient for normal virus protection. `extended`: This virus database extends the regular virus database with a large collection of "zoo" viruses that are no longer seen in recent virus studies. This database is suitable for an enhanced security environment.	`default`
`smtps-spamaction {discard | pass | tag}`	Select the action that this profile uses for filtered SMTPs email. Tagging appends custom text to the subject or header of email identified as spam. When `scan` or streaming mode (also called `splice`) is selected, the FortiGate unit can only discard spam email. Discard immediately drops the connection. Without streaming mode or scanning enabled, chose to discard, pass, or tag SMTPs spam. In the US Domestic distribution, streaming mode is permanently enabled for SMTPs, and the tag option is not available. • `discard`: Do not pass email identified as spam. • `pass`: Disable spam filtering for SMTPs traffic. • `tag`: Tag spam email with text configured using the `smtps-spamtagmsg` field and the location set using the `smtps-spamtagtype` field.	`discard`
`smtps-spamhdrip {enable | disable}`	Select to check header IP addresses for `spamfsip, spamrbl, and spamipbwl` filters.	`disable`
`smtps-spamtagmsg <message_str>`	Enter a word or phrase (tag) to affix to email identified as spam. When typing a tag, use the same language as the FortiGate unit's current administrator language setting. Tag text using other encodings may not be accepted. For example, when entering a spam tag that uses Japanese characters, first verify that the administrator language setting is Japanese; the FortiGate unit will not accept a spam tag written in Japanese characters while the administrator language setting is English. For details on changing the language setting, see "system global" on page 423. **Note:** To correctly enter the tag, your SSH or telnet client must also support your language's encoding. Alternatively, you can use the web-based manager's CLI widget to enter the tag. Tags must not exceed 64 bytes. The number of characters constituting 64 bytes of data varies by text encoding, which may vary by the FortiGate administrator language setting. Tags containing space characters, such as multiple words or phrases, must be surrounded by quote characters (`'`)to be accepted by the CLI.	`Spam`
`smtp-spamtagtype {header | subject} {spaminfo | }`	Select to affix the tag to either the MIME header or the subject line, and whether or not to append spam information to the spam header, when an email is detected as spam. Also configure `smtp-spamtagmsg`. If you select to affix the tag to the subject line, the FortiGate unit will convert the entire subject line, including tag, to UTF-8 by default. This improves display for some email clients that cannot properly display subject lines that use more than one encoding. For details on disabling conversion of subject line to UTF-8, see "system settings" on page 517.	`subject spaminfo`
`spambwordtable <index_int>`	Enter the ID number of the spamfilter banned word list to be used with the protection profile. This variable appears only on FortiGate-800 and above units.	`0`

Variable	Description	Default
spamemaddrtable <index_int>	Enter the ID number of the spamfilter email address list to be used with the protection profile. This variable appears only on FortiGate-800 and above units.	0
spamipbwltable <index_int>	Enter the ID number of the spamfilter IP address black/white list to be used with the protection profile. This variable appears only on FortiGate-800 and above units.	0
spamiptrusttable <index_int>	Enter the ID number of the spamfilter IP trust list to be used with the protection profile. This variable only appears on FortiGate-800 models and greater.	0
spammheadertable <index_int>	Enter the ID number of the spamfilter MIME header list to be used with the protection profile. This variable only appears on FortiGate-800 models and greater.	0
spamrbltable <index_int>	Enter the ID number of the spamfilter DNSBL list to be used with the protection profile. This variable only appears on FortiGate-800 models and greater.	0
spambwordthreshold <value_int>	If the combined scores of the banned word patterns appearing in an email message exceed the threshold value, the message will be processed according to the Spam Action setting.	10
webbwordtable <index_int>	Enter the ID number of the webfilter banned word list to be used with the protection profile. This variable only appears on FortiGate-800 models and greater.	0
webbwordthreshold <value_int>	Enter the maximum score a web page can have before being blocked. If the combined scores of the content block patterns appearing on a web page exceed the threshold value, the page will be blocked.	10
webexmwordtable <index_int>	Enter the ID number of the webfilter exempt word list to be used with the protection profile. This variable only appears on FortiGate-800 models and greater.	0
weburlfiltertable <index_int>	Enter the ID number of the webfilter URL filter list to be used with the protection profile. This variable appears only on FortiGate-800 models and greater.	0

Example

This example shows how to create a profile called `spammail`, using:

- filtering of email according to the email banned word list, the MIME header list, and the return DNS check, enable spam to be logged and tagged with the tag “Spam” in the subject for POP3 traffic
- filtering of email based on the DNSBL server, and discard messages identified as spam for SMTP traffic

```
config firewall profile
  edit spammail
    set pop3 spamemailbwl spamhdrcheck spamraddrdns
    set pop3-spamaction log tag
    set pop3-spamtagmsg Spam
    set pop3-spamtagtype subject
    set smtp spamrbl
    set smtp-spamaction discard
  end
```

This example shows how to add HTTP category blocking to the `spammail` profile created above, using:

- category blocking to deny access to web pages categorized as Games (20), Personals and Dating (37), Shopping and Auction (42) and the category group Objectionable or Controversial (g02)
- category monitoring to log access to web pages categorized as Computer Security (50) and the category group Potentially Bandwidth Consuming (g04)

```
config firewall profile
  edit spammail
    set ftgd-wf-deny 20 37 42 g02
    set ftgd-wf-log 50 g04
  end
```

config log

Use this command to write event log messages when the options that you have enabled in this protection profile perform an action. For example, if you enable antivirus protection you could also use the `config log` command to enable `log-av-block` so that the FortiGate unit writes an event log message every time a virus is detected.

Variable	Description	Default
`log-app-ctrl {enable | disable}`	Select to log application control.	`disable`
`log-av-block {enable | disable}`	Select to log file pattern or file type blocking.	`disable`
`log-av-oversize {enable | disable}`	Select to log oversize file and email blocking.	`disable`
`log-av-virus {enable | disable}`	Select to log viruses detected.	`disable`
`log-dlp {enable | disable}`	Select to log data leak protection.	`disable`
`log-ips {enable | disable}`	Select to log IPS events.	`disable`
`log-spam {enable | disable}`	Select to log spam detected.	`disable`
`log-web-content {enable | disable}`	Select to log web content blocking.	`disable`
`log-web-filter-activex {enable | disable}`	Select to log ActiveX plugin blocking.	`disable`
`log-web-filter-applet {enable | disable}`	Select to log Java applet blocking.	`disable`
`log-web-filter-cookie {enable | disable}`	Select to log cookie blocking.	`disable`
`log-web-ftgd-err {enable | disable}`	Select to log FortiGuard rating errors.	`enable`
`log-web-invalid-domain {enable | disable}`	Select to log URLs with invalid domain portion.	`enable`
`log-web-url {enable | disable}`	Select to log URL blocking.	`disable`

Example

This example shows how to enable writing event log messages when the following happens because of settings in the protection profile being configured:

- a virus is detected
- an MMS message is intercepted.

```
config firewall profile
  edit example
    config log
      set log-av-virus enable
      set log-intercept enable
    end
  end
```

config app-recognition

Use this subcommand to configure protocol recognition options to set the HTTPS content filtering mode and to

select the TCP port numbers that the protection profile monitors for the content protocols HTTP, HTTPS, SMTP, POP3, IMAP, NNTP, FTP, SMTPS, POP3S, and IMAPS.

By default the protection profile monitors the default content protocol port numbers (for example, port 80 for HTTP and so on). You can edit the settings for each content protocol and select to inspect all port numbers for that protocol or select one or more port numbers to monitor for that protocol.

Syntax

```
config firewall profile
  config app-recognition
    edit <ftp>
      set inspect-all {enable | disable}
      set port <port_number>
    edit <http>
      set inspect-all {enable | disable}
      set port <port_number>
    edit <https>
      set inspect-all {enable | disable}
      set port <port_number>
    edit <imap>
      set inspect-all {enable | disable}
      set port <port_number>
    edit <imaps>
      set inspect-all {enable | disable}
      set port <port_number>
    edit <nntp>
      set inspect-all {enable | disable}
      set port <port_number>
    edit <pop3>
      set inspect-all {enable | disable}
      set port <port_number>
    edit <pop3s>
      set inspect-all {enable | disable}
      set port <port_number>
    edit <smtp>
      set inspect-all {enable | disable}
```

```
    set port <port_number>
  edit <smtps>
    set inspect-all {enable | disable}
    set port <port_number>
```

Variable	Description	Default
<ftp>	Configure FTP recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for FTP protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for FTP protocol. Not available if inspect-all enabled.	21
<http>	Configure HTTP recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for HTTP protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for HTTP protocol. Not available if inspect-all enabled.	80
<https>	Configure HTTPS recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for HTTPS protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for HTTPS protocol. Not available if inspect-all enabled.	443
<imap>	Configure IMAP recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for IMAP protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for IMAP protocol. Not available if inspect-all enabled.	143
<imaps>	Configure IMAPS recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for IMAPS protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for IMAPS protocol. Not available if inspect-all enabled.	993
<nntp>	Configure NNTP recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for NNTP protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for NNTP protocol. Not available if inspect-all enabled.	119
<pop3>	Configure POP3 recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for POP3 protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for POP3 protocol.	110
<pop3s>	Configure POP3S recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for POP3S protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for POP3S protocol.	995
<smtp>	Configure SMTP recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for SMTP protocol.	disable

Variable	Description	Default
port <port_number>	Select the port number that the protection profile monitors for SMTP protocol.	25
<smtps>	Configure SMTPS recognition.	No default.
inspect-all {enable | disable}	Select to monitor all ports for SMTPS protocol.	disable
port <port_number>	Select the port number that the protection profile monitors for SMTPS protocol.	465

Example

Use the following example to monitor all ports for SMTPS protocol.

```
config firewall profile
  edit <profile_name>
    config app-recognition
      edit smtps
        set inspect-all enable
      end
  end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v2.80 MR2	Removed log option from imap-spamaction, pop3-spamaction, and smtp-spamaction fields.
FortiOS v2.80 MR3	Added splice option to ftp and smtp fields. Moved from config antivirus ftp service and config antivirus smtp service. Added chunkedbypass option to http field.
FortiOS v2.80 MR5	Added http_err_detail to cat_options field.
FortiOS v2.80 MR6	Removed buffer_to_disk variable from ftp, http, imap, pop3, and smtp fields. Added spamfeip option to imap, pop3, and smtp fields. Changed content_log option to content-archive for ftp, http, imap, pop3, and smtp fields.
FortiOS v2.80 MR7	Changed spamfeip option to spamfsip for the FortiShield Antispam Service. Added no-content-summary option to ftp, http, imap, pop3, and smtp fields.
FortiOS v2.80 MR8	Added spamfsurl for the FortiShield spam filter URL blacklist to imap, pop3, and smtp fields.
FortiOS v3.0	Added fields for FortiGuard. New options added for ftp, http, imap, pop3, smtp, imap-spamtagtype, pop3-spamtagtype, smtp-spamtagtype. Added fields for IM. Added new fields for IPS. Added new fields for logging. Added smtp-spamhdrip to profile. Added all IM and P2P options. Added client comforting and oversize file commands. Added NNTP-related commands. Added list selection commands for FortiGate-800 models and greater.
FortiOS v3.0 MR3	Added new options avquery and exemptword for HTTP. Removed options fileexempt, mail_log and spamfschksum from HTTP, POP3 and IMAP. Added new options archive-full, archive-summary and avquery for IMAP, POP3, and AIM. Removed options content-archive and fileexempt from IMAP and IM.
FortiOS v3.0 MR4	Added no-content-summary to AIM, ICQ, MSN, and Yahoo options. Removed transfer-log, from the same commands as it is not a feature.

FortiOS v3.0 MR4	Added VoIP config commands for `SCCP`, `Simple`, and `SIP` protocols. Added `associated-interface`, `nntpoversizelimit`, `imoversizechat`, `log-voip`, `log-voip-violations`, and `HTTPS` commands. Removed the following options and commands: `nntp-spamaction`, `nntp-spamtagtype`, `nntp-spamtagmsg`. Added `set smtp-spam-localoverride` command.
FortiOS v3.0 MR6	New option `redir-block` for variable `ftgd-wf-options`. Blocks HTTP redirects.
FortiOS v3.0 MR6	Removed variables `ips-signature` and `ips-anomaly`. IPS sensors, formerly signatures, are now configured by selecting a sensor name. Denial of service (DoS) sensors, formerly anomalies, are no longer configured in protection profiles.
FortiOS v3.0 MR6	New variables `ips-sensor-status` and `ips-sensor`. Enables IPS sensors, and selects the IPS sensor name.
FortiOS v3.0 MR6	Renamed variable `ips-log` to `log-ips`.
FortiOS v3.0 MR6	New option `block-long-chat` for variable `aim`. Blocks oversize chat messages.
FortiOS v3.0 MR6	Renamed options `content-full` and `content-meta` to `archive-full` and `archive-summary`, respectively, for the `msn`, `icq`, and `yahoo` variables.
FortiOS v3.0 MR6	Removed variable `ftgd-wf-ovrd-group`. Authorizing a group to perform web filtering overrides now occurs within group configuration.
FortiOS v3.0 MR6	New option `scanextended` for the `ftp` and `http` variables. Scans for viruses and worms using the extended database of virus definitions.
FortiOS v3.0 MR7	Renamed variable `allow-ssl-unknown-sess-id` to `block-ssl-unknown-sess-id`. Blocking of unknown session ID is now disabled by default.
FortiOS v3.0 MR7	Removed variables IMAP `spamhdrcheck`, `imap-spamaction`, `imap-spamtagmsg`, and `imap-spamtagtype`.
FortiOS v3.0 MR7	Added the new `config sip` subcommand field `reg-diff-port`.
FortiOS v3.0 MR7	Moved `config dupe`, `config flood`, `config log`, `config notification`, `config sccp`, `config simple`, and `config sip` into subcommand sections.
FortiOS 4.0	Moved fields `aim`, `bittorrent`, `bittorrent-limit`, `edonkey`, `edonkey-limit`, `gnutella`, `gnutella-limit`, `icq`, `imoversizechat`, `kazaa`, `kazaa-limit`, `msn`, `p2p`, `skype`, `winny`, `winny-limit`, `yahoo`, `log-antispam-mass-mms`, `log-av-endpoint-filter`, `log-im`, `log-p2p`, `log-voip`, `log-voip-violations` Added fields `application-list`, `application-list-status`, `dlp-sensor-table`, `httppostaction`, `httpsoversizelimet`, `https-deep-scan`, `https-retry-count`, `httpscomfortinterval`, `httpscomfortamount`, `imaps`, `imapsoversizelimit`, `nac-quar-expiry`, `nac-quar-infected`, `pop3s`, `pop3soversizelimit`, `smtps`, `smtpsoversizelimit`. Added syntax `config app-recognition`
FortiOS 4.0 MR1	Added fields `http-post-lang`, `log-web-invalid-domain`.

Related topics

- firewall policy, policy6
- alertemail
- antivirus
- ips
- webfilter

schedule onetime

Use this command to add, edit, or delete one-time schedules.

Use scheduling to control when policies are active or inactive. Use one-time schedules for policies that are effective once for the period of time specified in the schedule.

Note: To edit a schedule, define the entire schedule, including the changes. This means entering all of the schedule parameters, both those that are changing and those that are not.

Syntax

```
config firewall schedule onetime
  edit <name_str>
    set end <hh:mm> <yyyy/mm/dd>
    set start <hh:mm> <yyyy/mm/dd>
  end
```

Variable	Description	Default
<name_str>	Enter the name of this schedule.	No default.
end <hh:mm> <yyyy/mm/dd>	Enter the ending day and time of the schedule. • hh - 00 to 23 • mm - 00, 15, 30, or 45 • yyyy - 1992 to infinity • mm - 01 to 12 • dd - 01 to 31	00:00 2001/01/01
start <hh:mm> <yyyy/mm/dd>	Enter the starting day and time of the schedule. • hh - 00 to 23 • mm - 00, 15, 30, or 45 • yyyy - 1992 to infinity • mm - 01 to 12 • dd - 01 to 31	00:00 2001/01/01

Example

Use the following example to add a one-time schedule named Holiday that is valid from 5:00 pm on 3 September 2004 until 8:45 am on 7 September 2004.

```
config firewall schedule onetime
  edit Holiday
    set start 17:00 2004/09/03
    set end 08:45 2004/09/07
  end
```

History

FortiOS v2.80 Revised.

Related topics

- firewall policy, policy6
- firewall schedule recurring

schedule recurring

Use this command to add, edit, and delete recurring schedules used in firewall policies.

Use scheduling to control when policies are active or inactive. Use recurring schedules to create policies that repeat weekly. Use recurring schedules to create policies that are effective only at specified times of the day or on specified days of the week.

Note: If a recurring schedule is created with a stop time that occurs before the start time, the schedule starts at the start time and finishes at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next. To create a recurring schedule that runs for 24 hours, set the start and stop times to the same time.

Syntax

```
config firewall schedule recurring
  edit <name_str>
    set day <name_str>
    set end <hh:mm>
    set start <hh:mm>
  end
```

Variable	Description	Default
<name_str>	Enter the name of this schedule.	No default.
day <name_str>	Enter the names of one or more days of the week for which the schedule is valid. Separate multiple names with a space.	sunday
end <hh:mm>	Enter the ending time of the schedule. • hh can be 00 to 23 • mm can be 00, 15, 30, or 45 only	00:00
start <hh:mm>	Enter the starting time of the schedule. • hh can be 00 to 23 • mm can be 00, 15, 30, or 45 only	00:00

Example

This example shows how to add a recurring schedule named access so that it is valid Monday to Friday from 7:45 am to 5:30 pm.

```
config firewall schedule recurring
  edit access
    set day monday tuesday wednesday thursday friday
    set start 07:45
    set end 17:30
  end
```

Edit the recurring schedule named access so that it is no longer valid on Fridays.

```
config firewall schedule recurring
  edit access
    set day monday tuesday wednesday thursday
    set start 07:45
    set end 17:30
  end
```

History

FortiOS v2.80 Revised.

Related topics

- firewall policy, policy6
- firewall schedule onetime

schedule group

Use this command to configure schedule groups.

Syntax

```
config firewall schedule group
  edit <group-name_str>
    set member {<schedule1_name> [schedule2_name ...]}
  end
```

Variable	Description	Default
<group-name_str>	Enter the name of this schedule group.	No default.
member {<schedule1_name> [schedule2_name ...]}	Enter one or more names of one-time or recurring firewall schedules to add to the schedule group. Separate multiple names with a space. To view the list of available schedules enter set member ? at the prompt. Schedule names are case-sensitive.	No default.

History

FortiOS v4.0 MR1 New.

Related topics

- firewall schedule onetime
- firewall schedule recurring

service custom

Use this command to configure a firewall service that is not in the predefined service list.

Note: To display a list of all predefined service names, enter the command `get firewall service predefined ?`. To display a predefined service's details, enter the command `get firewall service predefined <service_str>`. For details, see "get firewall service predefined" on page 772.

Syntax

```
config firewall service custom
  edit <name_str>
    set comment <string>
    set icmpcode <code_int>
    set icmptype <type_int>
    set protocol {ICMP | IP | TCP/UDP}
    set protocol-number <protocol_int>
    set tcp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-
       <srcporthigh_int>]
    set udp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-
       <srcporthigh_int>]
  end
```

Variable	Description	Default
`<name_str>`	Enter the name of this custom service.	No default
`comment <string>`	Add comments for the custom service.	No default
`icmpcode <code_int>`	Enter the ICMP code number. Find ICMP type and code numbers at www.iana.org.	No default.
`icmptype <type_int>`	Enter the ICMP type number. The range for `type_int` is from 0-255. Find ICMP type and code numbers at www.iana.org.	`0`
`protocol {ICMP | IP | TCP/UDP}`	Enter the protocol used by the service.	`IP`
`protocol-number <protocol_int>`	For an IP service, enter the IP protocol number. For information on protocol numbers, see http://www.iana.org.	`0`
`tcp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<srcporthigh_int>]`	For TCP services, enter the destination and source port ranges. If the destination port range can be any port, enter `1-65535`. If the destination is only a single port, simply enter a single port number for `dstportlow_int` and no value for `dstporthigh_int`. If source port can be any port, no source port need be added. If the source port is only a single port, simply enter a single port number for `srcportlow_int` and no value for `srcporthigh_int`.	No default.
`udp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<srcporthigh_int>]`	For UDP services, enter the destination and source port ranges. If the destination port range can be any port, enter `1-65535`. If the destination is only a single port, simply enter a single port number for `dstportlow_int` and no value for `dstporthigh_int`. If source port can be any port, no source port need be added. If the source port is only a single port, simply enter a single port number for `srcportlow_int` and no value for `srcporthigh_int`.	No default.

Example

This example shows how to add a custom service called `Custom_1`. The service destination port range is TCP 4501 to 4503. The service can use any source port.

```
config firewall service custom
  edit Custom_1
    set protocol TCP/UDP
    set tcp-portrange 4501-4503
  end
```

A second example shows how to add a custom service called `Custom_2`. The service destination port range is TCP 4545 to 4550. The service uses source port 9620.

```
config firewall service custom
   edit Custom_1
    set protocol TCP/UDP
    set tcp-portrange 4545-4550:9620
  end
```

History

FortiOS v2.80	Revised.
FortiOS v3.00	The `portrange` command split into `tcp-portrange` and `udp-portrange`.
FortiOS v4.00	Added field `comment`.

Related topics

- firewall policy, policy6

service group

Use this command to configure firewall service groups.

To simplify policy creation, you can create groups of services and then add one policy to provide or block access for all the services in the group. A service group can contain predefined services and custom services in any combination. A service group cannot contain another service group.

Note: To edit a service group, enter all of the members of the service group, both those changing and those staying the same.

Syntax

```
config firewall service group
  edit <group-name_str>
    set comment
    set member <service_str>
  end
```

Variable	Description	Default
`<group-name_str>`	Enter the name of this service group.	No default.
`comment`	Add comments for this service group	No default.
`member <service_str>`	Enter one or more names of predefined or custom firewall services to add to the service group. Separate multiple names with a space. To view the list of available services enter `set member ?` at the prompt. `<service_str>` is case-sensitive.	No default.

Example

This example shows how to add a service group called `web_Services` that includes the FTP, HTTP, HTTPS, and Real Audio services.

```
config firewall service group
  edit web_Services
    set member FTP HTTP HTTPS RAUDIO
  end
```

This example shows how to add the TELNET service to the `web_Services` service group.

```
config firewall service group
  edit web_Services
    set member FTP HTTP HTTPS RAUDIO TELNET
  end
```

History

FortiOS v2.80 Revised.

FortiOS v4.00 Added field `comment`.

Related topics

- firewall policy, policy6

shaper per-ip-shaper

Use this command to configure traffic shaping that is applied per IP address, instead of per policy or per shaper. As with the shared traffic shaper, you select per-IP traffic shapers in firewall policies.

Syntax

```
config firewall shaper per-ip-shaper
  edit <name_str>
    set action {none | log | block}
    set bps <bandwidth>
    set quota <Mbytes>
    set type {hour | day | week | month}
    config iplist
      edit <index_int>
        end <address_ipv4>
        start <address_ipv4>
      end
end
```

Variable	Description	Default
<name_str>	Enter the name of the traffic shaper.	No default.
action {none | log | block}	Select the traffic shaper action for quotas: • none — do nothing. • log — generate a traffic accounting log for each time period selected in type. • block — block traffic that exceeds the quota and log the event.	none
bps <bandwidth>	Enter the maximum allowed bandwidth in Kbps. This limit applies to each IP address. Set to 0 to disable bandwidth limit.	0
quota <Mbytes>	Enter the traffic quota in Mbytes. This is available when action is block. Set quota to monitor and optionally block traffic that exceeds a set number of Mbytes during the time period configured by setting type.	0
type {hour | day | week | month}	If action is set to log, set the time period for generating traffic accounting logs. If action is block, set the time period for the quota.	hour
config iplist	Add one or more IP address ranges to the shaper to specify the IP addresses that the shaper shapes traffic for.	
<index_int>	Enter the unique ID number of this IP list.	No default.
end <address_ipv4>	Enter the ending IP address for the IP address range that this per-IP shaper shapes. To enter a single IP address, enter the address as both start and end.	0.0.0.0
start <address_ipv4>	Enter the starting IP address for the IP address range that this per-IP shaper shapes. To enter a single IP address, enter the address as both start and end.	0.0.0.0

Example

This example shows how to configure per-ip traffic shaping for traffic from IP address 172.20.120.2 and IP address range 192.168.20.10 to 192.168.20.20. The command sets the maximum allowed bandwidth that these address can consume to 10000 Kbps. The command also sets the quota for traffic from these IP addresses to 1000 Mbytes per day. Any traffic from these IP addresses that exceeds this quota is blocked.

```
config firewall shaper per-ip-shaper
```

```
edit per-ip-shaper1
  set bps 10000
  set action block
  set quota 1000
  set type day
  config iplist
    edit 1
      set start 172.20.120.2
      set end 172.20.120.2
    next
    edit 2
      set start 192.168.20.10
      set end 192.168.20.20
    end
end
```

History

FortiOS v4.00	New `config firewall traffic-shaper` command. Functionality moved out of the `config firewall policy` command.
FortiOS 4.0 MR1	New command.

Related topics

- firewall shaper traffic-shaper
- firewall policy, policy6
- firewall profile

shaper traffic-shaper

Use this command to configure shared traffic shaping that is applied to and shared by all traffic accepted by a firewall policy. As with the per-IP traffic shaper, you select shared traffic shapers in firewall policies.

Syntax

```
config firewall traffic-shaper
  edit <name_str>
    set action {none | log | block}
    set guaranteed-bandwidth <bandwidth_value>
    set maximum-bandwidth <bandwidth_value>
    set per-policy {enable | disable}
    set priority {high | low | medium}
    set quota <Mbytes>
    set type {hour | day | week | month}
  end
end
```

Variable	Description	Default
<name_str>	Enter the name of the traffic shaper.	No default.
action {none | log | block}	Select the traffic shaper action: • none — do nothing. • log — generate a traffic accounting log for each time period selected in type. • block — block traffic that exceeds the quota and log the event.	none
guaranteed-bandwidth <bandwidth_value>	Enter the amount of bandwidth guaranteed to be available for traffic controlled by the policy. bandwidth_value can be 0 to 2097000 Kbytes/second.	0
maximum-bandwidth <bandwidth_value>	Enter the maximum amount of bandwidth available for traffic controlled by the policy. bandwidth_value can be 0 to 2097000 Kbytes/second. If maximum bandwidth is set to 0 no traffic is allowed by the policy.	0
per-policy {enable | disable}	Enable or disable applying this traffic shaper to a single firewall policy that uses it.	disable
priority {high | low | medium}	Select the priority level for traffic controlled by the policy.	high
quota <Mbytes>	Enter the traffic quota in Mbytes. This is available when action is block. Set quota to monitor and optionally block traffic that exceeds a set number of Mbytes during the time period configured by setting type.	0
type {hour | day | week | month}	If action is set to log, set the time period for generating traffic accounting logs. If action is block, set the time period for the quota.	hour

Example

This example shows how to set traffic_shaper1's guaranteed bandwidth to 100000.

```
config firewall shaper traffic-shaper
  edit traffic_shaper1
    set guaranteed-bandwidth 100000
  end
```

History

FortiOS v4.00	New `config firewall traffic-shaper` command. Functionality moved out of the `config firewall policy` command.
FortiOS 4.0 MR1	The `config firewall traffic-shaper` command renamed `config firewall shaper traffic-shaper`. Added the `action`, `quota`, and `type` fields.

Related topics

- firewall shaper per-ip-shaper
- firewall policy, policy6
- firewall profile

sniff-interface-policy

Using this command you can add sniffer policies you can configure a FortiGate unit interface to operate as a one-arm intrusion detection system (IDS) appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets.

To configure one-arm IDS, you need to configure one or more FortiGate interfaces to operated in one-arm sniffer mode using the `ips-sniffer-mode` field of the `config system interface` command to configure an interface to operate in one-arm sniffer mode. See "system ips-sniffer-mode {enable | disable}" on page 455 When you configure an interface to operate in one-arm sniffer mode it cannot be used for any other purpose. For example, you cannot add firewall policies for the interface and you cannot add the interface to a zone.

Note: If you add VLAN interfaces to an interface configured for one-arm sniffer operation this VLAN interface also operates in one-arm sniffer mode and you can add sniffer policies for this VLAN interface.

After you have configured the interface for one-arm sniffer mode, connect the interface to a hub or to the SPAN port of a switch that is processing network traffic.

Then use the config firewall sniff-interface-policy command to add Sniffer policies for that FortiGate interface that include a DoS sensor, an IPS sensors, and an Application black/white list to detect attacks and other activity in the traffic that the FortiGate interface receives from the hub or switch SPAN port.

In one-arm sniffer mode, the interface receives packets accepted by sniffer mode policies only. All packets not received by sniffer model policies are dropped. All packets received by sniffer mode policies go through IPS inspection and are dropped after then are analyzed by IPS.

One-arm IDS cannot block traffic. However, if you enable logging in the DoS and IPS sensors and the application black/white lists, the FortiGate unit records log messages for all detected attacks and applications.

The `sniff-interface-policy` command is applied to IPv4 addresses. For IPv6 addresses, use `sniff-interface-policy6` instead.

Syntax

```
config firewall sniff-interface-policy
  edit <policy_id>
    set application-list-status {enable | disable}
    set application_list <app_list_str>
    set interface <int_str>
    set ips-DoS-status {enable | disable}
    set ips-DoS <DoS_str>
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set service <service_str>
    set srcaddr <srcaddr_ipv4>
    set status {enable | disable}
end
```

Variable	Description	Default
application-list-status {enable | disable}	Enable to have the FortiGate unit apply an application black/white list to matching network traffic.	disable
application_list <app_list_str>	Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when application-list-status is set to enable.	
dstaddr <dstaddr_ipv4>	Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range.	
interface <int_str>	The interface or zone to be monitored.	
ips-DoS-status {enable | disable}	Enable to have the FortiGate unit examine network traffic for DoS sensor violations.	disable
ips-DoS <DoS_str>	Enter the name of the DoS sensor the FortiGate unit will use when examining network traffic. This option is available only when ips-DoS-status is set to enable.	
ips-sensor-status {enable | disable}	Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities.	disable
ips-sensor <sensor_str>	Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when ips-sensor-status is set to enable.	
service <service_str>	Enter a service to limit traffic monitoring to only the selected type. You may also specify a service group, or multiple services separated by spaces.	
srcaddr <srcaddr_ipv4>	Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range.	
status {enable | disable}	Enable or disable the sniffer policy. A disabled sniffer policy has no effect on network traffic.	enable

Example

This example shows how to add a sniffer policy that examines all traffic received by port10 with source and destination addresses matching Subnet_1 and Subnet_2 and for any service. The policy applies an application control list and an IPS sensor to the traffic.

```
config firewall sniff-interface-policy
  edit 1
    set interface port10
    set srcaddr Subnet_1
    set dstaddr Subnet_2
    set service ANY
    set application-list-status enable
    set application-list App_list_1
    set ips-sensor-status enable
    set ips-sensor mySensor
  end
```

History

FortiOS v4.0 MR1 New.

Related commands

- firewall sniff-interface-policy6
- firewall interface-policy
- firewall interface-policy6
- firewall policy, policy6
- firewall profile

sniff-interface-policy6

Using this command you can add sniffer policies you can configure a FortiGate unit interface to operate as a one-arm intrusion detection system (IDS) appliance for IPv6 traffic by sniffing packets for attacks without actually receiving and otherwise processing the packets.

To configure one-arm IDS, you need to configure one or more FortiGate interfaces to operated in one-arm sniffer mode using the `ips-sniffer-mode` field of the `config system interface` command to configure an interface to operate in one-arm sniffer mode. See "system ips-sniffer-mode {enable | disable}" on page 455 When you configure an interface to operate in one-arm sniffer mode it cannot be used for any other purpose. For example, you cannot add firewall policies for the interface and you cannot add the interface to a zone.

Note: If you add VLAN interfaces to an interface configured for one-arm sniffer operation this VLAN interface also operates in one-arm sniffer mode and you can add sniffer policies for this VLAN interface.

After you have configured the interface for one-arm sniffer mode, connect the interface to a hub or to the SPAN port of a switch that is processing network traffic.

Then use the config firewall sniff-interface-policy command to add Sniffer policies for that FortiGate interface that include a DoS sensor, an IPS sensors, and an Application black/white list to detect attacks and other activity in the traffic that the FortiGate interface receives from the hub or switch SPAN port.

In one-arm sniffer mode, the interface receives packets accepted by sniffer mode policies only. All packets not received by sniffer model policies are dropped. All packets received by sniffer mode policies go through IPS inspection and are dropped after then are analyzed by IPS.

One-arm IDS cannot block traffic. However, if you enable logging in the IPS sensors and the application black/white lists, the FortiGate unit records log messages for all detected attacks and applications.

The `interface-policy6` command is used for DoS policies applied to IPv6 addresses. For IPv4 addresses, use `interface-policy` instead.

Syntax

```
config firewall interface-policy
  edit <policy_id>
    set application_list <app_list_str>
    set application_list <app_list_str>
    set dstaddr6 <dstaddr_ipv6>
    set interface
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set service6 <service_str>
    set srcaddr6 <srcaddr_ipv6>
    set status {enable | disable}
end
```

Variable	Description	Default
`application-list-status {enable | disable}`	Enable to have the FortiGate unit apply an application black/white list to matching network traffic.	`disable`
`application_list <app_list_str>`	Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when `application-list-status` is set to `enable`.	

Variable	Description	Default
dstaddr6 <dstaddr_ipv6>	Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range.	
interface	The interface or zone to be monitored.	
ips-sensor-status {enable | disable}	Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities.	disable
ips-sensor <sensor_str>	Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when ips-sensor-status is set to enable.	
service6 <service_str>	Enter a service to limit traffic monitoring to only the selected type. You may also specify a service group, or multiple services separated by spaces.	
srcaddr6 <srcaddr_ipv6>	Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range.	
status {enable | disable}	Enable or disable the DoS policy. A disabled DoS policy has no effect on network traffic.	enable

Example

This example shows how to add an IPv6 sniffer policy that examines all IPv6 traffic received by port10 with source and destination addresses matching Subnet_1 and Subnet_2 and for any service. The policy applies an application control list and an IPS sensor to the traffic.

```
config firewall sniff-interface-policy6
  edit 1
    set interface port10
    set srcaddr Subnet_1
    set dstaddr Subnet_2
    set service ANY
    set application-list-status enable
    set application-list App_list_1
    set ips-sensor-status enable
    set ips-sensor mySensor
  end
```

History

FortiOS v4.0 MR1 New.

Related commands

- firewall sniff-interface-policy
- firewall interface-policy
- firewall interface-policy6
- firewall policy, policy6
- firewall profile

ssl setting

Use this command to configure SSL proxy settings so that you can apply antivirus scanning, web filtering, FortiGuard web filtering, spam filtering, data leak prevention (DLP), and content archiving to HTTPS, IMAPS, POP3S, and SMTPS traffic by using the `config firewall profile` command.

To perform SSL content scanning and inspection, the FortiGate unit does the following:

- intercepts and decrypts HTTPS, IMAPS, POP3S, and SMTPS sessions between clients and servers (FortiGate SSL acceleration speeds up decryption)
- applies content inspection to decrypted content, including:
  - HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP., and content archiving
  - HTTPS web filtering and FortiGuard web filtering
  - IMAPS, POP3S, and SMTPS spam filtering
  - re-encrypts the sessions and forwards them to their destinations.

Syntax

```
config firewall ssl setting
  set caname <certificate_str>
  set cert-cache-capacity <capacity_integer>
  set cert-cache-timeout <timeout_integer>
  set proxy-connect-timeout <timeout_integer>
  set session-cache-capacity <capacity_integer>
  set session-cache-timeout <port_int>
  set ssl-dh-bits {1024 | 1536 | 2048 | 768}
  set ssl-max-version {ssl-3.0 | tls-1.0}
  set ssl-min-version {ssl-3.0 | tls-1.0}
  set ssl-send-empty-frags {enable | disable}
end
```

Variable	Description	Default
`caname <certificate_str>`	Select the CA certificate used by SSL content scanning and inspection for establishing encrypted SSL sessions.	`Fortinet_CA_SSLProxy`
`cert-cache-capacity <capacity_integer>`	Enter the capacity of the host certificate cache. The range is from 0 to 200.	`100`
`cert-cache-timeout <timeout_integer>`	Enter the time limit to keep the certificate cache. The range is from 1 to 120 minutes.	`10`
`proxy-connect-timeout <timeout_integer>`	Enter the time limit to make an internal connection to the appropriate proxy process (1 - 60 seconds).	`30`
`session-cache-capacity <capacity_integer>`	Enter the capacity of SSL session cache (0 - 1000).	`500`
`session-cache-timeout <port_int>`	Enter the time limit in minutes to keep the SSL session.	`20`
`ssl-dh-bits {1024 | 1536 | 2048 | 768}`	Select the size of Diffie-Hellman prime used in DHE_RSA negotiation.	`1024`
`ssl-max-version {ssl-3.0 | tls-1.0}`	Select the highest SSL/TLS version to negotiate.	`tls-1.0`
`ssl-min-version {ssl-3.0 | tls-1.0}`	Select the lowest SSL/TLS version to negotiate.	`ssl-3.0`
`ssl-send-empty-frags {enable | disable}`	Enable or disable sending empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only).	`enable`

Example

This example shows how to add a signing CA certificate to the SSL content scanning and inspection configuration. Use the following CLI command if the certificate name is Example_CA.

```
config firewall ssl setting
  set caname Example_CA
end
```

The Example_CA signing CA certificate will now be used by SSL content scanning and inspection for establishing encrypted SSL sessions.

History

FortiOS v4.00 New.

Related topics

- firewall policy, policy6
- firewall profile

vip

Use this command to configure virtual IPs and their associated address and port mappings (NAT).

Virtual IPs can be used to allow connections through a FortiGate unit using network address translation (NAT) firewall policies. Virtual IPs can use proxy ARP so that the FortiGate unit can respond to ARP requests on a network for a server that is actually installed on another network. Proxy ARP is defined in RFC 1027.

For example, you can add a virtual IP to an external FortiGate unit interface so that the external interface can respond to connection requests for users who are actually connecting to a server on the DMZ or internal network.

Depending on your configuration of the virtual IP, its mapping may involve port address translation (PAT), also known as port forwarding or network address port translation (NAPT), and/or network address translation (NAT) of IP addresses.

If you configure NAT in the virtual IP and firewall policy, the NAT behavior varies by your selection of:

- static vs. dynamic NAT mapping
- the dynamic NAT's load balancing style, if using dynamic NAT mapping
- full NAT vs. destination NAT (DNAT)

The following table describes combinations of PAT and/or NAT that are possible when configuring a firewall policy with a virtual IP.

Static NAT	Static, one-to-one NAT mapping: an external IP address is always translated to the same mapped IP address. If using IP address ranges, the external IP address range corresponds to a mapped IP address range containing an equal number of IP addresses, and each IP address in the external range is always translated to the same IP address in the mapped range.
Static NAT with Port Forwarding	Static, one-to-one NAT mapping with port forwarding: an external IP address is always translated to the same mapped IP address, and an external port number is always translated to the same mapped port number. If using IP address ranges, the external IP address range corresponds to a mapped IP address range containing an equal number of IP addresses, and each IP address in the external range is always translated to the same IP address in the mapped range. If using port number ranges, the external port number range corresponds to a mapped port number range containing an equal number of port numbers, and each port number in the external range is always translated to the same port number in the mapped range.
Load Balancing	Dynamic, one-to-many NAT mapping: an external IP address is translated to one of the mapped IP addresses. For each session, a load balancing algorithm dynamically selects an IP address from the mapped IP address range to provide more even traffic distribution. The external IP address is not always translated to the same mapped IP address.
Load Balancing with Port Forwarding	Dynamic, one-to-many NAT mapping with port forwarding: an external IP address is translated to one of the mapped IP addresses. For each session, a load balancing algorithm dynamically selects an IP address from the mapped IP address range to provide more even traffic distribution. The external IP address is not always translated to the same mapped IP address.
Dynamic Virtual IPs	Dynamic, many-to-few or many-to-one NAT mapping: if you set the external IP address of a virtual IP to 0.0.0.0, the interface maps traffic destined for any IP address, and is dynamically translated to a mapped IP address or address range.

Server Load Balancing	Dynamic, one-to-many NAT mapping: an external IP address is translated to one of the mapped IP addresses, as determined by the selected load balancing algorithm for more even traffic distribution. The external IP address is not always translated to the same mapped IP address. Server load balancing requires that you configure at least one “real” server, but can use up to eight (8) real servers per virtual IP (VIP). Real servers can be configured with health check monitors. Health check monitors can be used to gauge server responsiveness before forwarding packets.
Server Load Balancing with Port Forwarding	Dynamic, one-to-many NAT mapping with port forwarding: an external IP address is translated to one of the mapped IP addresses, as determined by the selected load balancing algorithm for more even traffic distribution.The external IP address is not always translated to the same mapped IP address. Server load balancing requires that you configure at least one “real” server, but can use up to eight (8) real servers per virtual IP (VIP). Real servers can be configured with health check monitors. Health check monitors can be used to gauge server responsiveness before forwarding packets.

Note: If the NAT check box is not selected when building the firewall policy, the resulting policy does not perform full (source and destination) NAT; instead, it performs destination network address translation (DNAT).
For inbound traffic, DNAT translates packets’ destination address to the mapped private IP address, but does not translate the source address. The private network is aware of the source’s public IP address. For reply traffic, the FortiGate unit translates packets’ private network source IP address to match the destination address of the originating packets, which is maintained in the session table.

The following limitations apply when adding virtual IPs, Load balancing virtual servers, and load balancing real servers. Load balancing virtual servers are actually server load balancing virtual IPs. You can add server load balance virtual IPs from the CLI.

- Virtual IP `extip` entries or ranges cannot overlap with each other.
- A virtual IP `mappedip` cannot be 0.0.0.0 or 255.255.255.255.
- A real server `IP` cannot be 0.0.0.0 or 255.255.255.255.
- If a static NAT virtual IP `extip` is 0.0.0.0, the `mappedip` must be a single IP address.
- If a load balance virtual IP `extip` is 0.0.0.0, the `mappedip` can be an address range.
- When port forwarding, the count of `mappedport` and `extport` numbers must be the same. The web-based manager does this automatically but the CLI does not.
- Virtual IP names must be different from firewall address or address group names.

Syntax

```
config firewall vip
  edit <name_str>
    set arp-reply {enable | disable}
    set comment <comment_str>
    set extintf <name_str>
    set extip <address_ipv4>
    set extport <port_int>
    set gratuitous-arp-interval <interval_seconds>
    set http-cookie-age <age_int>
    set http-cookie-domain <domain_str>
    set http-cookie-generation <generation_int>
    set http-cookie-path <path_str>
    set http-cookie-share {disable | same-ip}
    set http-ip-header {enable | disable}
    set http-multiplex {enable | disable}
    set https-cookie-secure {disable | enable}
```

```
    set id <id_num_str>
    set ldb-method {first-alive | least-rtt | least-session | round-robin |
       static | weighted}
    set mappedip [<start_ipv4>-<end_ipv4>]
    set mappedport <port_int>
    set max-embryonic-connections <initiated_int>
    set monitor <name_str>
    set nat-source-vip {enable | disable}
    set outlook-web-access {disable | enable}
    set persistence {none | ssl-session-id | http-cookie(http)
    set portforward {enable | disable}
    set protocol {tcp | udp}
    set server-type {http | https | ip | ssl | tcp | udp}
    set ssl-mode {full | half}
    set ssl-certificate <certificate_str>
    set ssl-client-session-state-max <sessionstates_int>
    set ssl-client-session-state-timeout <timeout_int>
    set ssl-client-session-state-type {both | client | disable | time}
    set ssl-dh-bits <bits_int>
    set ssl-http-location-conversion {enable | disable}
    set ssl-http-match-host {enable | disable}?
    set ssl-max-version {ssl-3.0 | tls-1.0}
    set ssl-min-version {ssl-3.0 | tls-1.0}
    set ssl-send-empty-frags {enable | disable}
    set ssl-server-session-state-max <sessionstates_int>
    set ssl-server-session-state-timeout <timeout_int>
    set ssl-server-session-state-type {both | count | disable | time}
    set type {load-balance | server-load-balance | static-nat}
    config realservers
      edit <table_id>
        set client-ip <ip_range_str>
        set healthcheck {enable | disable}
        set holddown-interval <seconds_int>
        set ip <server_ip>
        set max-connections <connection_integer>
        set monitor <healthcheck_str>
        set port <port_ip>
        set status {active | disable | standby}
        set weight <loadbalanceweight_int>
      end
end
```

Variable	Description	Default
<name_str>	Enter the name of this virtual IP address.	No default.
arp-reply {enable | disable}	Select to respond to ARP requests for this virtual IP address.	enable
comment <comment_str>	Enter comments relevant to the configured virtual IP.	No default
extintf <name_str>	Enter the name of the interface connected to the source network that receives the packets that will be forwarded to the destination network. The interface name can be any FortiGate network interface, VLAN subinterface, IPSec VPN interface, or modem interface.	No default.

Variable	Description	Default
extip <address_ipv4>	Enter the IP address on the external interface that you want to map to an address on the destination network. If type is static-nat and mappedip is an IP address range, the FortiGate unit uses extip as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. To configure a dynamic virtual IP that accepts connections destined for any IP address, set extip to 0.0.0.0.	0.0.0.0
extport <port_int>	Enter the external port number that you want to map to a port number on the destination network. This option only appears if portforward is enabled, or if type is server-load-balance. If portforward is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set extport to the first port number in the range. Then set mappedport to the start and end of the destination port range. The FortiGate unit automatically calculates the end of the extport port number range. To configure a dynamic virtual IP that accepts connections for any port, set extport to 0. If type is server-load-balance, extport is available unless server-type is ip. The value of extport changes to 80 if server-type is http and to 443 if server-type is https.	0
gratuitous-arp-interval <interval_seconds>	Configure sending of ARP packets by a virtual IP. You can set the time interval between sending ARP packets. Set the interval to 0 to disable sending ARP packets.	0
http-cookie-age <age_int>	Configure HTTP cookie persistence to change how long the browser caches the cookie. Enter an age in minutes or set the age to 0 to make the browser keep the cookie indefinitely. The range is 0 to 525600 minutes. This option is available when type is server-load-balance, server-type is http or https and persistence is http or https. See “How server load balancing HTTP cookie persistence fields work” on page 200.	60
http-cookie-domain <domain_str>	Configure HTTP cookie persistence to restrict the domain that the cookie should apply to. Enter the DNS domain name to restrict the cookie to. This option is available when type is server-load-balance, server-type is http or https and persistence is http or https. See “How server load balancing HTTP cookie persistence fields work” on page 200.	
http-cookie-generation <generation_int>	Configure HTTP cookie persistence to invalidate all cookies that have already been generated. The exact value of the generation is not important, only that it is different from any generation that has already been used. This option is available when type is server-load-balance, server-type is http or https and persistence is http or https. See “How server load balancing HTTP cookie persistence fields work” on page 200.	0
http-cookie-path <path_str>	Configure HTTP cookie persistence to limit the cookies to a particular path, for example /new/path. This option is available when type is server-load-balance, server-type is http or https and persistence is http or https. See “How server load balancing HTTP cookie persistence fields work” on page 200.	

Variable	Description	Default
`http-cookie-share {disable | same-ip}`	Configure HTTP cookie persistence to control the sharing of cookies across more than one virtual server. The default setting `same-ip` means that any cookie generated by one virtual server can be used by another virtual server in the same virtual domain. Select `disable` to make sure that a cookie generated for a virtual server cannot be used by other virtual servers. This options is available when `type` is `server-load-balance`, `server-type` is `http` or `https` and persistence is `http` or `https`. See "How server load balancing HTTP cookie persistence fields work" on page 200.	`same-ip`
`http-ip-header {enable | disable}`	Select to preserve the client's IP address in the `X-Forwarded-For` HTTP header line. This can be useful if you require logging on the server of the client's original IP address. If this option is not selected, the header will contain the IP address of the FortiGate unit. This option appears only if `portforward` and `http` are `enable`.	`disable`
`http-multiplex {enable | disable}`	Select to use the FortiGate unit to multiplex multiple client connections into a few connections between the FortiGate unit and the real server. This can improve performance by reducing server overhead associated with establishing multiple connections. The server must be HTTP/1.1 compliant. This option is only available if `server-type` is `http` or `https`.	`disable`
`https-cookie-secure {disable | enable}`	Configure HTTP cookie persistence to enable or disable using secure cookies for HTTPS sessions. Secure cookies are disabled by default because they can interfere with cookie sharing across HTTP and HTTPS virtual servers. If enabled, then the `Secure` tag is added to the cookie inserted by the FortiGate unit. This option is available when `type` is `server-load-balance`, `server-type` is `http` or `https` and persistence is `http` or `https`. See "How server load balancing HTTP cookie persistence fields work" on page 200.	`disable`
`id <id_num_str>`	Enter a unique identification number for the configured virtual IP. Not checked for uniqueness. Range 0 - 65535.	No default.

Variable	Description	Default
`ldb-method {first-alive | least-rtt | least-session | round-robin | static | weighted}`	Select the method used by the virtual server to distribute sessions to the real servers. You add real servers to the virtual server using `config realservers`. • `first-alive`: Always directs requests to the first alive real server. In this case "first" refers to the order of the real servers in the virtual server configuration. For example, if you add real servers A, B and C in that order, then traffic always goes to A as long as it is alive. If A goes down then traffic goes to B and if B goes down the traffic goes to C. If A comes back up, traffic goes to A. Real servers are ordered in the virtual server configuration in the order in which you add them, with the most recently added real server last. If you want to change the order you must delete and re-add real servers as required. • `least-rtt:` Directs requests to the real server with the least round trip time. The round trip time is determined by a Ping monitor and is defaulted to 0 if no Ping monitors are defined. • `least-session`: Directs requests to the real server that has the least number of current connections. This method works best in environments where the real servers or other equipment you are load balancing have similar capabilities. • `round-robin:` Directs request to the next real server, and treats all real servers as equals regardless of response time or number of connections. Unresponsive real servers are avoided. A separate real server is required. • `static:` Distributes sessions evenly across all real servers according to the session source IP address. This load balancing method provides some persistence because all sessions from the same source address would always go to the same server. However, the distribution is stateless, so if a real server is added or removed (or goes up or down) the distribution is changed so persistence will be lost. Separate real servers are not required. • `weighted:` Real servers with a higher weight value receive a larger percentage of connections at any one time. Server weights can be set in `config realservers set weight` This option appears only if `type` is `server-load-balance`.	`static`
`mappedip [<start_ipv4>-<end_ipv4>]`	Enter the IP address or IP address range on the destination network to which the external IP address is mapped. If `type` is `static-nat` and `mappedip` is an IP address range, the FortiGate unit uses `extip` as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. If `type` is `load-balance` and `mappedip` is an IP address range, the FortiGate unit uses `extip` as a single IP address to create a one-to-many mapping.	`0.0.0.0`
`mappedport <port_int>`	Enter the port number on the destination network to which the external port number is mapped. You can also enter a port number range to forward packets to multiple ports on the destination network. For a static NAT virtual IP, if you add a map to port range the FortiGate unit calculates the external port number range.	`0`
`max-embryonic-connections <initiated_int>`	Enter the maximum number of partially established SSL or HTTP connections. This should be greater than the maximum number of connections you want to establish per second. This option appears only if `portforward` is enable, and `http` is `enable or ssl is not off`.	`1000`
`monitor <name_str>`	Select the health check monitor for use when polling to determine a virtual server's connectivity status.	No default.
`nat-source-vip {enable | disable}`	Enable `nat-source-vip` to prevent unintended servers from using this virtual IP.	`disable`

Variable	Description	Default
`outlook-web-access {disable | enable}`	If the FortiGate unit provides SSL offload for Microsoft Outlook Web Access then the Outlook server expects to see a `Front-End-Https: on` header inserted into the HTTP headers as described in this Microsoft Technical Note. If `outlook-web-access` is enabled FortiGate unit adds this header to all HTTP requests. This options is available when `type` is `server-load-balance`, `server-type` is `http` or `https`.	`disable`
`persistence {none | ssl-session-id | http-cookie(http) http https ssl`	If the `type` is `server-load-balance`, configure persistence for a virtual server to make sure that clients connect to the same server every time they make a request that is part of the same session. When you configure persistence, the FortiGate unit load balances a new session to a real server according to the `ldb-method`. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server. You can configure persistence if `server-type` is set to `http`, `https`, or `ssl`. • `none`: No persistence. Sessions are distributed solely according to the `ldb-method`. Setting `ldb-method` to `static` (the default) results in behavior equivalent to persistence. See the description of `static` in "firewall ldb-method {first-alive | least-rtt | least-session | round-robin | static | weighted}" on page 194 for more information. • `http-cookie`: all HTTP or HTTPS sessions with the same HTTP session cookie are sent to the same real server. `http-cookie` is available if `server-type` is set to `https` or `ssl`. If you select `http-cookie` you can also configure `http-cookie-domain`, `http-cookie-path`, `http-cookie-generation`, `http-cookie-age`, and `http-cookie-share` for HTTP and these settings plus `https-cookie-secure` for HTTPS. • `ssl-session-id`: all sessions with the same SSL session ID are sent to the same real server. `ssl-session-id` is available if `server-type` is set to `https` or `ssl`.	`none`
`portforward {enable | disable}`	Select to enable port forwarding. You must also specify the port forwarding mappings by configuring `extport` and `mappedport`.	`disable`
`protocol {tcp | udp}`	Select the protocol, TCP or UDP, to use when forwarding packets.	`tcp`

Variable	Description	Default
`server-type {http | https | ip | ssl | tcp | udp}`	If the `type` is `server-load-balance`, select the protocol to be load balanced by the virtual server (also called the server load balance virtual IP). If you select a general protocol such as `ip`, `tcp`, or `udp` the virtual server load balances all IP, TCP, or UDP sessions. If you select specific protocols such as `http`, `https`, or `ssl` you can apply additional server load balancing features such as persistence and HTTP multiplexing. • `http`: load balance only HTTP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced. You can also configure `http-multiplex`. You can also set `persistence` to `http-cookie` and configure `http-cookie-domain`, `http-cookie-path`, `http-cookie-generation`, `http-cookie-age`, and `http-cookie-share` settings for cookie persistence. • `https`: load balance only HTTPS sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced. You can also configure `http-multiplex` and set `persistence` to `http-cookie` and configure the same `http-cookie` options as for `http` virtual servers plus the `https-cookie-secure` option. You can also set `persistence` to `ssl-session-id`. You can also configure the SSL options such as `ssl-mode` and `ssl-certificate` and so on. `https` is available on FortiGate units that support SSL acceleration. • `ip`: load balance all sessions accepted by the firewall policy that contains this server load balance virtual IP. Since all sessions are load balanced you don't have to set the `extport`. • `ssl`: load balance only SSL sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced. You can also configure the SSL options such as `ssl-mode` and `ssl-certificate` and so on. • `tcp`: load balance only TCP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced. • `udp`: load balance only UDP sessions with destination port number that matches the `extport` setting. Change `extport` to match the destination port of the sessions to be load balanced.	(none)

Variable	Description	Default
ssl-mode {full | half}	Select whether or not to accelerate SSL communications with the destination by using the FortiGate unit to perform SSL operations, and indicate which segments of the connection will receive SSL offloading. Accelerating SSL communications in this way is also called SSL offloading. • full: Select to apply SSL acceleration to both parts of the connection: the segment between the client and the FortiGate unit, and the segment between the FortiGate unit and the server. The segment between the FortiGate unit and the server will use encrypted communications, but the handshakes will be abbreviated. This results in performance which is less than the option half, but still improved over communications without SSL acceleration, and can be used in failover configurations where the failover path does not have an SSL accelerator. If the server is already configured to use SSL, this also enables SSL acceleration without requiring changes to the server's configuration. • half: Select to apply SSL only to the part of the connection between the client and the FortiGate unit. The segment between the FortiGate unit and the server will use clear text communications. This results in best performance, but cannot be used in failover configurations where the failover path does not have an SSL accelerator. SSL 3.0 and TLS 1.0 are supported. This option appears only if server-type is ssl, and only on FortiGate models that support SSL acceleration.	full
ssl-certificate <certificate_str>	Enter the name of the SSL certificate to use with SSL acceleration. This option appears only if type is server-load-balance and server-type is ssl.	No default.
ssl-client-session-state-max <sessionstates_int>	Enter the maximum number of SSL session states to keep for the segment of the SSL connection between the client and the FortiGate unit. This option appears only if type is server-load-balance and server-type is ssl.	1000
ssl-client-session-state-timeout <timeout_int>	Enter the number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the FortiGate unit. This option appears only if type is server-load-balance and server-type is ssl.	30
ssl-client-session-state-type {both | client | disable | time}	Select which method the FortiGate unit should use when deciding to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate unit. • both: Select to expire SSL session states when either ssl-client-session-state-max or ssl-client-session-state-timeout is exceeded, regardless of which occurs first. • count: Select to expire SSL session states when ssl-client-session-state-max is exceeded. • disable: Select to keep no SSL session states. • time: Select to expire SSL session states when ssl-client-session-state-timeout is exceeded. This option appears only if type is server-load-balance and server-type is ssl.	both
ssl-dh-bits <bits_int>	Enter the number of bits of the prime number used in the Diffie-Hellman exchange for RSA encryption of the SSL connection. Larger prime numbers are associated with greater cryptographic strength. This option appears only if type is server-load-balance and server-type is ssl.	1024

Variable	Description	Default
ssl-http-location-conversion {enable | disable}	Select to replace http with https in the reply's Location HTTP header field. For example, in the reply, Location: http://example.com/ would be converted to Location: https://example.com/ . This option appears only if type is server-load-balance and server-type is https.	disable
ssl-http-match-host {enable | disable}	Select to apply Location conversion to the reply's HTTP header only if the host name portion of Location matches the request's Host field, or, if the Host field does not exist, the host name portion of the request's URI. If disabled, conversion occurs regardless of whether the host names in the request and the reply match. For example, if host matching is enabled, and a request contains Host: example.com and the reply contains Location: http://example.cc/, the Location field does not match the host of the original request and the reply's Location field remains unchanged. If the reply contains Location: http://example.com/, however, then the FortiGate unit detects the matching host name and converts the reply field to Location: https://example.com/ . This option appears only if ssl-http-location-conversion is enable.	disable
ssl-max-version {ssl-3.0 | tls-1.0}	Enter the maximum version of SSL/TLS to accept in negotiation. This option appears only if type is server-load-balance and server-type is ssl.	tls-1.0
ssl-min-version {ssl-3.0 | tls-1.0}	Enter the minimum version of SSL/TLS to accept in negotiation. This option appears only if type is server-load-balance and server-type is ssl.	ssl-3.0
ssl-send-empty-frags {enable | disable}	Select to precede the record with empty fragments to thwart attacks on CBC IV. You might disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments. This option appears only if type is server-load-balance and server-type is ssl, and applies only to SSL 3.0 and TLS 1.0.	enable
ssl-server-session-state-max <sessionstates_int>	Enter the maximum number of SSL session states to keep for the segment of the SSL connection between the server and the FortiGate unit. This option appears only if ssl-mode is full.	1000
ssl-server-session-state-timeout <timeout_int>	Enter the number of minutes to keep the SSL session states for the segment of the SSL connection between the server and the FortiGate unit. This option appears only if ssl-mode is full.	30
ssl-server-session-state-type {both | count | disable | time}	Select which method the FortiGate unit should use when deciding to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate unit. • both: Select to expire SSL session states when either ssl-server-session-state-max or ssl-server-session-state-timeout is exceeded, regardless of which occurs first. • count: Select to expire SSL session states when ssl-server-session-state-max is exceeded. • disable: Select to keep no SSL session states. • time: Select to expire SSL session states when ssl-server-session-state-timeout is exceeded. This option appears only if ssl-mode is full.	both

Variable	Description	Default
type {load-balance | server-load-balance | static-nat}	Select the type of static or dynamic NAT applied by the virtual IP. • load-balance: Dynamic NAT load balancing with server selection from an IP address range. • server-load-balance: Dynamic NAT load balancing with server selection from among up to eight realservers, determined by your selected load balancing algorithm and server responsiveness monitors. • static-nat: Static NAT.	static-nat
realservers The following commands are the options for config realservers, and are available only if type is server-load-balance.		
client-ip <ip_range_str>	Enter the IP address of the client in the X-Forwarded-For HTTP header. This can be useful if you require logging on the server of the client's original IP address. If this is not selected, the header will contain the IP address of the FortiGate unit.	No default.
<table_id>	Enter an index number used to identify the server that you are configuring. You can configure a maximum number of eight (8) servers in a server load balancing cluster.	No default.
healthcheck {enable | disable}	Enable to check the responsiveness of the server before forwarding traffic. You must also configure monitor.	disable
holddown-interval <seconds_int>	Enter the amount of time in seconds that the health check monitor will continue to monitor the status of a server whose status is active after it has been detected to be unresponsive. • If the server is detected to be continuously responsive during this interval, a server whose status is standby will be removed from current use and replaced with this server, which will again be used by server load balanced traffic. In this way, server load balancing prefers to use servers whose status is active, if they are responsive. • If the server is detected to be unresponsive during the first holddown interval, the server will remain out of use for server load balanced traffic, the health check monitor will double the holddown interval once, and continue to monitor the server for the duration of the doubled holddown interval. The health check monitor continues to monitor the server for additional iterations of the doubled holddown interval until connectivity to the server becomes reliable, at which time the holddown interval will revert to the configured interval, and the newly responsive server whose status is active will replace the standby server in the pool of servers currently in use. In effect, if the status of a server is active but the server is habitually unresponsive, the health check monitor is less likely to restore the server to use by server load balanced traffic until the server's connectivity becomes more reliable. This option applies only to real servers whose status is active, but have been detected to be unresponsive ("down").	300
ip <server_ip>	Enter the IP address of a server in this server load balancing cluster.	0.0.0.0
max-connections <connection_integer>	Enter the limit on the number of active connections directed to a real server. If the maximum number of connections is reached for the real server, the FortiGate unit will automatically switch all further connection requests to another server until the connection number drops below the specified limit. 0 means unlimited number of connections.	0

Variable	Description	Default
monitor <healthcheck_str>	Enter one or more names of health check monitor settings to use when performing a health check, separating each name with a space. If any of the configured health check monitors detect failures, the FortiGate unit will deem the server unresponsive, and will not forward traffic to that server. For details on configuring health check monitor settings, see "firewall ldb-monitor" on page 125. This option appears only if healthcheck is enable.	No default.
port <port_ip>	Enter the port used if port forwarding is enabled.	10
status {active | disable | standby}	Select whether the server is in the pool of servers currently being used for server load balanced traffic, the server is on standby, or is disabled. • active: The FortiGate unit may forward traffic to the server unless its health check monitors determine that the server is unresponsive, at which time the FortiGate unit will temporarily use a server whose status is standby. The healthcheck monitor will continue to monitor the unresponsive server for the duration of holddown-interval. If this server becomes reliably responsive again, it will be restored to active use, and the standby server will revert to standby. For details on health check monitoring when an active server is unresponsive, see "holddown-interval <seconds_int>" on page 199. • disable: The FortiGate unit will not forward traffic to this server, and will not perform health checks. You might use this option to conserve server load balancing resources when you know that a server will be unavailable for a long period, such as when the server is down for repair. • standby: If a server whose status is active becomes unresponsive, the FortiGate unit will temporarily use a responsive server whose status is standby until the server whose status is active again becomes reliably responsive. If multiple responsive standby servers are available, the FortiGate unit selects the standby server with the greatest weight. If a standby server becomes unresponsive, the FortiGate unit will select another responsive server whose status is standby.	active
weight <loadbalanceweight_int>	Enter the weight value of a specific server. Servers with a greater weight receive a greater proportion of forwarded connections, or, if their status is standby, are more likely to be selected to temporarily replace servers whose status is active, but that are unresponsive. Valid weight values are between 1 and 255. This option is available only if ldb-method is weighted.	1

How server load balancing HTTP cookie persistence fields work

The following options are available for the config firewall vip command when type is set to server-load-balance, server-type is set to http or https and persistence is set to http-cookie:

```
http-cookie-domain
http-cookie-path
http-cookie-generation
http-cookie-age
http-cookie-share
https-cookie-share (appears when server-type is set to https)
```

When HTTP cookie persistence is enabled the FortiGate unit inserts a header of the following form into each HTTP response unless the corresponding HTTP request already contains a FGTServer cookie:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
   Max-Age=3600
```

The value of the FGTServer cookie encodes the server that traffic should be directed to. The value is encoded so as to not leak information about the internal network.

Use http-cookie-domain to restrict the domain that the cookie should apply to. For example, to restrict the cookie to .server.com, enter:

```
set http-cookie-domain .server.com
```

Now all generated cookies will have the following form:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
   Domain=.server.com; Max-Age=3600
```

Use http-cookie-path to limit the cookies to a particular path. For example, to limit cookies to the path /sales, enter:

```
set http-cookie-path /sales
```

Now all generated cookies will have the following form:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
   Domain=.server.com; Path=/sales; Max-Age=3600
```

Use http-cookie-age to change how long the browser caches the cookie. You can enter an age in minutes or set the age to 0 to make the browser keep the cookie indefinitely:

```
set http-cookie-age 0
```

Now all generated cookies will have the following form:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
   Domain=.server.com; Path=/sales
```

Use http-cookie-generation to invalidate all cookies that have already been generated. The exact value of the generation is not important, only that it is different from any generation that has already been used for cookies in this domain. The simplest approach is to increment the generation by one each time invalidation is required. Since the default is 0, enter the following to invalidate all existing cookies:

```
set http-cookie-generation 1
```

Use http-cookie-share {disable | same-ip} to control the sharing of cookies across virtual servers in the same virtual domain. The default setting same-ip means that any FGTServer cookie generated by one virtual server can be used by another virtual server in the same virtual domain. For example, if you have an application that starts on HTTP and then changes to HTTPS and you want to make sure that the same server is used for the HTTP and HTTPS traffic then you can create two virtual servers, one for port 80 (for HTTP) and one for port 443 (for HTTPS). As long as you add the same real servers to both of these virtual servers (and as long as both virtual servers have the same number of real servers with the same IP addresses), then cookies generated by accessing the HTTP server are reused when the application changes to the HTTPS server.

If for any reason you do not want this sharing to occur then select disable to make sure that a cookie generated for a virtual server cannot be used by other virtual servers.

Use https-cookie-secure to enable or disable using secure cookies. Secure cookies are disabled by default because secure cookies can interfere with cookie sharing across HTTP and HTTPS virtual servers. If enabled, then the Secure tag is added to the cookie inserted by the FortiGate unit:

```
Set-Cookie: FGTServer=E7D01637C4B08E89A6714213A9D85D9C7E4D8158; Version=1;
   Max-Age=3600; Secure
```

Static NAT virtual IP examples

This example shows how to add a static NAT virtual IP named Web_Server that allows users on the Internet to connect to a single web server on the private network. The public IP address of the web server is 64.32.21.34 and the IP address of the web server on the internal network is 192.168.1.44.

```
config firewall vip
  edit Web_Server
```

```
    set extintf external
    set extip 64.32.21.34
    set mappedip 192.168.1.44
  end
```

This example shows how to edit the static NAT virtual IP named Web_Server to change the IP address of the web server on the internal network to 192.168.110.23.

```
config firewall vip
  edit web_Server
    set mappedip 192.168.110.23
  end
```

This example shows how to add a static NAT port forwarding virtual IP that uses port address translation to allow external access to a web server on the private network if there is no separate external IP address for the web server. In this example, the IP address of the external interface is 192.168.100.99 and the real IP address of the web server on the internal network is 192.168.1.93.

```
config firewall vip
  edit web_Server
    set portforward enable
    set extintf external
    set extip 192.168.100.99
    set extport 80
    set mappedip 192.168.1.93
    set mappedport 80
  end
```

This example shows how to enter a static NAT virtual IP named Server_Range that allows Internet users to connect to a range of 10 virtual IP addresses on the Internet and have the IP addresses in this range mapped to a range of IP addresses on the DMZ network. The DMZ network contains 10 servers with IP addresses from 10.10.10.20 to 10.10.10.29. The Internet IP addresses for these servers are in the range 219.34.56.10 to 219.34.56.19. In this example you do not have to enter the external IP address range. Instead you enter the first IP address in the external IP address range and the FortiGate unit calculates the end of the IP address range based on the number of IP addresses defined by the mapped IP address range. Also in the example, port2 is connected to the Internet.

```
config firewall vip
  edit Server_Range
    set extintf port2
    set extip 219.34.56.10
    set mappedip 10.10.10.20 10.10.10.19
  end
```

Load balancing virtual IP example

This example shows how to enter a load balancing virtual IP named Ext_Load_Balance that allows Internet users to connect to a single virtual IP address on the Internet and have that IP address mapped to a range of IP addresses on the network connected to port5. You might use a configuration such as this to load balance connections from the Internet to an internal server farm. In the example the Internet is connected to port2 and the virtual IP address is 67.34.56.90 and the IP address range on the network connected to port5 is 172.20.120.10 to 172.20.120.30.

```
config firewall vip
  edit Ext_Load_Balance
    set type load-balance
    set extintf port2
    set extip 67.34.56.90
    set mappedip 172.20.120.10-172.20.120.30
  end
```

Server load balancing virtual IP examples

This example shows how to add a server load balancing virtual IP that load balances all traffic among 3 real servers. In the example the Internet is connected to `port2` and the virtual IP address of the virtual server is 192.168.20.20. The load balancing method is `weighted`. The IP addresses of the real servers are 10.10.10.1, 10.10.10.2, and 10.10.10.3. The weights for the real servers are 1, 2, and 3. The default weight is 1 and does not have to be changed for the first real server.

```
config firewall vip
  edit All_Load_Balance
    set type server-load-balance
    set server-type ip
    set extintf port2
    set extip 192.168.20.20
    set ldb-method weighted
      config realservers
        edit 1
          set ip 10.10.10.1
        next
        edit 2
          set ip 10.10.10.2
          set weight 2
        next
        edit 3
          set ip 10.10.10.3
          set weight 3
        end
  end
```

This example shows how to add two server load balancing virtual IPs named `Http_Load_Balance` that load balances HTTP traffic using port 8080 and `Https_Load_Balance` that load balances HTTPS traffic using port 443. The Internet is connected to `port2` and the virtual IP address of the virtual server is 192.168.20.20. Both server load balancing virtual IPs load balance sessions to the same three real servers with IP addresses 10.10.10.2, 10.10.10.2, and 10.10.10.3. The real servers provide HTTP and HTTPS services. For both virtual servers, `persistence` is set to `http-cookie` to enable HTTP cookie persistence. Also for both virtual servers, `http-cookie-domain` is set to `.example.org` because HTTP cookie persistence is just required for the `example.org` domain.

First, the configuration for the HTTP virtual IP:

```
config firewall vip
  edit Http_Load_Balance
    set type server-load-balance
    set server-type http
    set extport 8080
    set extintf port2
    set extip 192.168.20.20
    set persistence http-cookie
    set http-cookie-domain .example.org
      config realservers
        edit 1
          set ip 10.10.10.1
        next
        edit 2
          set ip 10.10.10.2
        next
        edit 3
```

```
        set ip 10.10.10.3
      end
  end
```

Second, the configuration for the HTTPS virtual IP. In this configuration you don't have to set `extport` to `443` because `extport` is automatically set to `443` when `server-type` is set to `https`.

```
config firewall vip
  edit Https_Load_Balance
    set type server-load-balance
    set server-type https
    set extport 443
    set extintf port2
    set extip 192.168.20.20
    set persistence http-cookie
    set http-cookie-domain .example.org
      config realservers
        edit 1
          set ip 10.10.10.1
        next
        edit 2
          set ip 10.10.10.2
        next
        edit 3
          set ip 10.10.10.3
        end
  end
```

History

FortiOS v2.80	Revised.
FortiOS v3.00	Revised.
FortiOS v3.00	Added `server-load-balance` to set type.
FortiOS v3.0 MR4	Added the following commands and options: `config realserver`.
FortiOS v3.0 MR5	`extintf <name_str>` variable now accepts modem interface names. Formerly, it accepted a network interface, VLAN subinterface, or IPSec VPN virtual interface.
FortiOS v3.0 MR6	New variables `monitor` and `healthcheck`. Enables health checking for real servers and specifies which of the health check settings to use.
FortiOS v3.0 MR6	New variables: • `ssl`, `ssl-certificate` • `ssl-client-session-state-max` • `ssl-client-session-state-timeout` • `ssl-client-session-state-type` • `ssl-dh-bits` • `ssl-http-location-conversion` • `ssl-http-match-host` • `ssl-max-version` • `ssl-min-version` • `ssl-send-empty-frags` • `ssl-server-session-state-max` • `ssl-server-session-state-timeout` • `ssl-server-session-state-type` Enables SSL acceleration by offloading SSL operations from the destination to the FortiGate unit, and configures various aspects of the offloading, including to which segment(s) of the connection the FortiGate unit will apply SSL, and what encryption strength and other options to use.

FortiOS v3.0 MR6	New variable `max-embryonic-connections`. Specifies the maximum number of partially established SSL or HTTP connections when the virtual IP is performing HTTP multiplexing or SSL offloading.
FortiOS v3.0 MR6	New variable `http`. Enables multiplexing of port forwarded HTTP connections into a few connections to the destination.
FortiOS v3.0 MR6	New variable `http-ip-header`. Preserves the original client's IP address in the `X-Forwarded-For` HTTP header line when using HTTP multiplexing.
FortiOS v3.0 MR6	New variable `status` in `config realservers` subcommand. Designates each server as an active or standby member of the server load balanced cluster, or disables the cluster member.
FortiOS v3.0 MR6	New variable `holddown-interval` in `config realservers` subcommand. Configures the amount of time during which a previously unresponsive server must remain responsive in order for the FortiGate unit to resume forwarding traffic to the server. If the server is unresponsive during this interval, the FortiGate unit continues to use a standby server.
FortiOS v3.0 MR7	New variables `comment` and `id`, Customer requirement for unique identifier and descriptive information relevant to virtual IP. Removed `ssl-max-version/ssl-min-version tls-1.1` option. TLS 1.1 is not supported. Added new variable `nat-source-vip`.
FortiOS v4.0	New variables added: `server-type, persistence, gratuitous-arp-interval, monitor`. New variables `client-ip` and `max-connections` in `config realservers` subcommand. New variables added: `http-cookie-age`, `http-cookie-domain`, `http-cookie-generation`, `http-cookie-path`, `http-cookie-share`, `https-cookie-secure`, and `outlook-web-access`. Renamed variable `ssl` to `ssl-mode`. Renamed variable `http` to `http-multiplex`. Removed variables `dead-interval`, `ping-detect`, and `wake-interval` in `config realservers` subcommand.
FortiOS v4.0 MR1	Added more information to the definition of the `first-alive` option.

Related topics

- firewall policy, policy6
- firewall ldb-monitor
- firewall vipgrp

vipgrp

You can create virtual IP groups to facilitate firewall policy traffic control. For example, on the DMZ interface, if you have two email servers that use Virtual IP mapping, you can put these two VIPs into one VIP group and create one external-to-DMZ policy, instead of two policies, to control the traffic.

Firewall policies using VIP Groups are matched by comparing both the member VIP IP address(es) and port number(s).

Syntax

```
config firewall vipgrp
  edit <name_str>
    set interface <name_str>
    set member <virtualip_str>
  end
```

Variable	Description	Default
`<name_str>`	Enter the name of the virtual IP group.	No default.
`interface <name_str>`	Enter the name of the interface to which the virtual IP group will be bound.	No default.
`member <virtualip_str>`	Enter one or more virtual IPs that will comprise the virtual IP group.	No default.

Example

```
config firewall vipgrp
  edit group_one
    set interface internal
    set member vipone viptwo vipthree
  end
```

History

FortiOS v3.0 MR4 Command `vipgrp` added.

Related topics

- firewall policy, policy6
- vip

gui

This chapter covers the commands to restore web-based manager CLI console and topology viewer.

This chapter contains the following sections:

console

Use this command to configure the web-based manager CLI console. When VDOMs are enabled, this command is part of the global commands.

Syntax

```
config gui console
  set preferences <filedata>
end
```

To obtain base-64 encoded data from a configured CLI console, use:

```
show gui console
```

Variable	Description	Default
`preferences <filedata>`	Base-64 encoded file to upload containing the commands to set up the web-based manager CLI console on the FortiGate unit.	No default

Example

This example shows how to upload the data file `pref-file` containing commands to set up the web-based manager CLI console on the FortiGate unit.

```
config gui console
  set preferences pref-file
end
```

History

FortiOS v3.00 MR5 New.

topology

Use this command to configure the web-based manager topology viewer. This command is not available when virtual domains are enabled.

Syntax

```
config gui topology
  set background-image <filedatabackground>
  set database <filedatabase>
  set preferences <filedatapref>
end
```

To obtain base-64 encoded data from a configured topology viewer, use:

```
show gui topology
```

Variable	Description	Default
`background-image <filedatabackground>`	Base-64 encoded file to upload containing the commands to set up the background image of the web-based manager topology viewer.	
`database <filedatabase>`	Base-64 encoded file to upload containing the data used to set up the web-based manager topology viewer.	
`preferences <filedatapref>`	Base-64 encoded file to upload containing the commands to set the preferences of the web-based manager topology viewer.	

Example

This example shows how to upload the data file (topguifile) containing commands to set up the topology GUI on the FortiGate unit and the background image (backgroundfile).

```
config gui topology
  set preferences topguifile
  set background-image backgroundfile
end
```

History

FortiOS v3.00 MR5 New.

imp2p

Use imp2p commands to configure user access to Instant Messaging and Peer-to-Peer applications, and to configure a global policy for unknown users who might use these applications.

This chapter contains the following sections:

aim-user

Use this command to permit or deny a specific user the use of AOL Instant Messenger.

Syntax

```
config imp2p aim-user
  edit <name_str>
    set action {deny | permit}
  end
```

Variable	Description	Default
name_str	The name of the AIM user.	
action {deny | permit}	Permit or deny the use of AOL Instant Messenger by this user.	deny

Example

This example shows how to add user_1 and permit the user to use the AIM protocol if the policy is set to allow AOL Instant Messenger.

```
config imp2p aim-user
  edit user_1
    set action permit
  end
```

History

FortiOS v3.0 New

Related topics

- imp2p icq-user
- imp2p msn-user
- imp2p old-version
- imp2p policy
- imp2p yahoo-user

icq-user

Use this command to permit or deny a specific user the use of ICQ Instant Messenger.

Syntax

```
config imp2p icq-user
  edit <name_str>
    set action {deny | permit}
  end
```

Variable	Description	Default
name_str	The name of the ICQ user.	
action {deny | permit}	Permit or deny the use of the ICQ Instant Messenger by this user.	deny

Example

This example shows how to add user_1 and permit the user to use the ICQ protocol if the policy is set to allow ICQ Instant Messenger.

```
config imp2p icq-user
  edit user_1
    set action permit
  end
```

History

FortiOS v3.0 New

Related topics

- imp2p aim-user
- imp2p msn-user
- imp2p old-version
- imp2p policy
- imp2p yahoo-user

msn-user

Use this command to permit or deny a specific user the use of MSN Messenger.

Syntax

```
config imp2p msn-user
  edit <name_str>
    set action {deny | permit}
  end
```

Variable	Description	Default
name_str	The name of the MSN user.	
action {deny | permit}	Permit or deny the use of MSN Messenger by this user.	deny

Example

This example shows how to add user_1 and permit the user to use the MSN protocol if the policy is set to allow MSN Messenger.

```
config imp2p msn-user
  edit user_1
    set action permit
  end
```

History

FortiOS v3.0 New

Related topics

- imp2p aim-user
- imp2p icq-user
- imp2p old-version
- imp2p policy
- imp2p yahoo-user

old-version

Some older versions of IM protocols are able to bypass file blocking because the message types are not recognized. The following command provides the option to disable these older IM protocol versions. Supported IM protocols include:

- MSN 6.0 and above
- ICQ 4.0 and above
- AIM 5.0 and above
- Yahoo 6.0 and above

Syntax

```
config imp2p old-version
  set aim {best-effort | block}
  set icq {best-effort | block}
  set msn {best-effort | block}
  set yahoo {best-effort | block}
end
```

Variable	Description	Default
`aim {best-effort | block}`	Enter `block` to block the session if the version is too old. Enter `best-effort` to inspect the session based on the policy.	block
`icq {best-effort | block}`	Enter `block` to block the session if the version is too old. Enter `best-effort` to inspect the session based on the policy.	block
`msn {best-effort | block}`	Enter `block` to block the session if the version is too old. Enter `best-effort` to inspect the session based on the policy.	block
`yahoo {best-effort | block}`	Enter `block` to block the session if the version is too old. Enter `best-effort` to inspect the session based on the policy.	block

Example

This example shows how to block older versions of MSN Messenger and inspect older versions of Yahoo Messenger.

```
config imp2p old-version
  set msn block
  set yahoo best-effort
end
```

History

FortiOS v3.0 New

Related topics

- imp2p aim-user
- imp2p icq-user
- imp2p msn-user
- imp2p policy
- imp2p yahoo-user

policy

Use this command to create a global policy for instant messenger applications. If an unknown user attempts to use one of the applications, the user can either be permitted use and added to a white list, or be denied use and added to a black list.

Note: In FortiOS 4.0, the imp2p settings are now part of Application Control. When creating a new VDOM, the default imp2p policy settings are set to allow, thereby permitting the settings in Application Control to drive the configuration.

Syntax

```
config imp2p policy
  set aim {allow | deny}
  set icq {allow | deny}
  set msn {allow | deny}
  set yahoo {allow | deny}
end
```

Variable	Description	Default
`aim {allow | deny}`	Allow an unknown user and add the user to the white list. Deny an unknown user and add the user to the black list.	`allow`
`icq {allow | deny}`	Allow an unknown user and add the user to the white list. Deny an unknown user and add the user to the black list.	`allow`
`msn {allow | deny}`	Allow an unknown user and add the user to the white list. Deny an unknown user and add the user to the black list.	`allow`
`yahoo {allow | deny}`	Allow an unknown user and add the user to the white list. Deny an unknown user and add the user to the black list.	`allow`

Example

This example shows how to configure the IM/P2P policy to allow AOL Instant Messenger, MSN Messenger, and Yahoo Messenger but deny ICQ Instant Messenger.

```
config imp2p policy
  set aim allow
  set msn allow
  set icq deny
  set yahoo allow
end
```

History

FortiOS v3.0 New

FortiOS v4.0 Configuration of imp2p policy is now CLI only. Default value is `allow` for all imp2p policy commands.

Related topics

- imp2p aim-user
- imp2p icq-user
- imp2p msn-user
- imp2p old-version
- imp2p yahoo-user

yahoo-user

Use this command to permit or deny a specific user the use of Yahoo Messenger.

Syntax

```
config imp2p yahoo-user
  edit <name_str>
    set action {deny | permit}
  end
```

Variable	Description	Default
name_str	The name of the Yahoo user.	
action {deny | permit}	Permit or deny the use of Yahoo Messenger by this user.	deny

Example

This example shows how to add user_1 and permit the user to use the Yahoo protocol if the policy is set to allow Yahoo Messenger.

```
config imp2p yahoo-user
  edit user_1
    set action permit
  end
```

History

FortiOS v3.0 New

Related topics

- imp2p aim-user
- imp2p icq-user
- imp2p msn-user
- imp2p old-version
- imp2p policy

ips

Use ips commands to configure IPS sensors to define which signatures are used to examine traffic and what actions are taken when matches are discovered. DoS sensors can also be defined to examine traffic for anomalies

For more information about IPS see the *FortiGate UTM User Guide*.

This chapter contains the following sections:

Note: If the IPS test can't find the destination MAC address, the peer interface will be used. To ensure packets get IPS inspection, there must be a Peer Interface. Both interfaces must be in the same VDOM, and one interface cannot be both the peer and original interface. For information on how to set the Peer Interface see "interface" on page 448.

DoS

FortiGate Intrusion Protection uses Denial of Service (DoS) sensors to identify network traffic anomalies that do not fit known or preset traffic patterns. Four statistical anomaly types for the TCP, UDP, and ICMP protocols can be identified.

Flooding	If the number of sessions targeting a single destination in one second is over a threshold, the destination is experiencing flooding.
Scan	If the number of sessions from a single source in one second is over a threshold, the source is scanning.
Source session limit	If the number of concurrent sessions from a single source is over a threshold, the source session limit is reached.
Destination session limit	If the number of concurrent sessions to a single destination is over a threshold, the destination session limit is reached.

Enable or disable logging for each anomaly, and select the action taken in response to detecting an anomaly. Configure the anomaly thresholds to detect traffic patterns that could represent an attack.

Note: It is important to estimate the normal and expected traffic on the network before changing the default anomaly thresholds. Setting the thresholds too low could cause false positives, and setting the thresholds too high could allow some attacks.

The list of anomalies can be updated only when the FortiGate firmware image is upgraded.

config limit

Access the `config limit` subcommand using the `config ips anomaly <name_str>` command. Use this command for session control based on source and destination network address. This command is available for `tcp_src_session`, `tcp_dst_session`, `icmp_src_session`, `icmp_dst_session`, `udp_src_session`, `udp_dst_session`.

The `default` entry cannot be edited. Addresses are matched from more specific to more general. For example, if thresholds are defined for 192.168.100.0/24 and 192.168.0.0/16, the address with the 24 bit netmask is matched before the entry with the 16 bit netmask.

Syntax

```
config ips DoS
  edit <sensor_str>
    set comment <comment_str>
    config anomaly
      edit <anomaly_str>
        set status {enable | disable}
        set log {enable | disable}
        set action {block | pass}
        set quarantine {attacker | both | interface | none}
        set threshold <threshold_int>
      end
  end
```

Variable	Description	Default
`<sensor_str>`	Enter the name of the sensor you want to configure. Enter a new name to create a sensor.	
`comment <comment_str>`	Enter a description of the DoS sensor. This is displayed in the DoS sensor list. Descriptions with spaces must be enclosed in quotation marks.	

Variable	Description	Default
<anomaly_str>	Enter the name of the anomaly you want to configure. Display a list of the available anomaly types by entering '?'.	
status {enable | disable}	Enable or disable the specified anomaly in the current DoS sensor.	disable
log {enable | disable}	Enable or disable logging of the specified anomaly in the current DoS sensor.	enable
action {block | pass}	Pass or block traffic in which the specified anomaly is detected.	pass
quarantine {attacker | both | interface | none}	To prevent the attacker from continuing to attack the FortiGate unit, you can quarantine the attacker to the banned user list in one of three ways. • Enter attacker to block all traffic sent from the attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected. • Enter both to block all traffic sent from the attacker's IP address to the target (victim's) IP address. Traffic from the attacker's IP address to addresses other than the victim's IP address is allowed. The attacker's and target's IP addresses are added to the banned user list as one entry. • Enter interface to block all traffic from connecting to the FortiGate unit interface that received the attack. The interface is added to the banned user list. • Enter none to disable the adding of addresses to the quarantine but the current DoS sensor.	none
threshold <threshold_int>	Enter the number of times the specified anomaly must be detected in network traffic before the action is triggered. Range 1 to 2 147 483 647.	varies by anomaly

Examples

This example shows how to create a DoS sensor and enable blocking of the udp_flood anomaly with the default threshold.

```
config ips DoS
  edit test
    set comment "This is for test"
    config anomaly
      edit udp_flood
        set action block
        set status enable
    end
end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v3.0	Added severity, default-action, and default-severity.
FortiOS v3.0 MR5	Under the config limit command, set ipaddress was removed. dst-ip, service, and src-ip commands were added.
FortiOS v3.0 MR6	Completely revised. Anomalies now defined in DoS sensors allowing the creation of multiple sensors to tailor behavior depending on traffic source, destination, and port, if required.
FortiOS v4.0	Added the quarantine option. Removed the config address tree. Addresses are now specified in the DoS policy.

Related topics

- ips custom
- ips global
- ips fail-open {enable | disable}

custom

Create custom IPS signatures and add them to IPS sensors.

Custom signatures provide the power and flexibility to customize FortiGate Intrusion Protection for diverse network environments. The FortiGate predefined signatures cover common attacks. If an unusual or specialized application or an uncommon platform is being used, add custom signatures based on the security alerts released by the application and platform vendors.

Use custom signatures to block or allow specific traffic.

The custom signature settings are configured when it is defined as a signature override in an IPS sensor. This way, a single custom signature can be used in multiple sensors with different settings in each. See "ips sensor" on page 228 for details.

For more information on custom signature syntax see the *FortiGate IPS Custom Signatures Technical Bulletin*.

Note: Custom signatures are an advanced feature. This document assumes the user has previous experience writing intrusion detection signatures.

Syntax

```
config ips custom
  edit <sig_str>
    set signature <signature_str>
  end
```

Variable	Description	Default
sig_str	The name of the custom signature.	
signature <signature_str>	Enter the custom signature. The signature must be enclosed in single quotes.	No default.

Example

This example shows how to add a custom signature.

```
config ips custom
  edit bad_things
    set signature 'F-SBID (--protocol tcp; --flow bi_direction;
       --pattern "bad things"; --no_case)'
  end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v3.0 MR6	Removed all options except signature. Other settings are configured when specifying the signature in a signature override.

Related topics

- ips global
- execute backup
- execute restore
- ips fail-open {enable | disable}

decoder

The Intrusion Protection system looks for certain types of traffic on specific ports. Using the decoders command, you can change ports if your configuration uses non-standard ports.

Syntax

```
config ips decoder <decoder_str>
    set port_list <port_int>
  end
```

Variable	Description	Default
<decoder_str>	Enter the name of the decoder. Enter '?' for a list.	
port_list <port_int>	Enter the ports which the decoder will examine. Multiple ports can be specified by separating them with commas and enclosing the list in quotes.	varies by decoder

Example

This example shows how to modify the dns_decoder to examine ports 1, 2, and 3 instead of the default 53.

```
config ips decoder dns_decoder
  set port_list "1,2,3"
end
```

global

Use this command to ignore sessions after a set amount of traffic has passed.

Syntax

```
config ips global
  set algorithm {engine-pick | high | low}
  set anomaly-mode {continuous | periodical}
  set engine-count <integer>
  set fail-open {enable | disable}
  set ignore-session-bytes <byte_integer>
  set session-limit-mode {accurate | heuristic}
  set socket-size <ips_buffer_size>
  set traffic-submit {enable | disable}
end
```

Variable	Description	Default
`algorithm {engine-pick | high | low}`	The IPS engine has two methods to determine whether traffic matches signatures. • `high` is a faster method that uses more memory • `low` is a slower method that uses less memory • `engine-pick` allows the IPS engine to choose the best method on the fly.	`engine-pick`
`anomaly-mode {continuous | periodical}`	Enter `continuous` to start blocking packets once attack starts. Enter `periodical` to allow configured number of packets per second.	`continuous`
`engine-count <integer>`	Enter the number of intrusion protection engines to run. Multi-processor FortiGate units can more efficiently process traffic with multiple engines running. When set to the default value of `0`, the FortiGate unit determines the optimal number of intrusion protection engines.	`0`
`fail-open {enable | disable}`	If for any reason the IPS should cease to function, it will fail open by default. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved.	`enable`
`ignore-session-bytes <byte_integer>`	Set the number of bytes after which the session is ignored.	`204800`
`session-limit-mode {accurate | heuristic}`	Enter `accurate` to accurately count the concurrent sessions. This option demands more resources. Enter `heuristic` to heuristically count the concurrent sessions.	heuristic
`socket-size <ips_buffer_size>`	Set intrusion protection buffer size. The default value is correct in most cases.	model-dependent
`traffic-submit {enable | disable}`	Submit attack characteristics to FortiGuard Service	`disable`

Examples

This example shows how to set intrusion protection to ignore sessions after 204800 bytes.

```
config ips global
  set ignore-session-bytes 204800
end
```

This example shows how to see the current configuration of ips global.

```
# get ips global
```

```
anomaly-mode        : continuous
engine-count        : 0
fail-open           : enable
ignore-session-bytes: 204800
session-limit-mode  : heuristic
socket-size         : 8 (MB)
traffic-submit      : disable
```

History

FortiOS v3.0	New.
FortiOS v3.0 MR4	Merged `get ips global` including example.
FortiOS v3.0 MR6	Removed the `ip-protocol` option.
FortiOS v4.0.0	Added `algorithm`.

Related topics

- execute backup
- execute restore
- ips fail-open {enable | disable}

rule

The IPS sensors use signatures to detect attacks. These signatures can be listed with the rules command. Details about the default settings of each signature can also be displayed.

Syntax

```
config ips rule <rule_str>
  get
```

Variable	Description	Default
<rule_str>	Enter the name of a signature. For a complete list of the predefined signatures, enter '?' instead of a signature name.	

Example

This example shows how to display the current configuration of the Apache.Long.Header.DoS signature.

```
# config ips rule Apache.Long.Header.DoS
(Apache.Long.He~d) # get
name                : Apache.Long.Header.DoS
status              : enable
log                 : enable
log-packet          : disable
action              : pass
group               : web_server
severity            : medium
location            : server
os                  : Windows, Linux, BSD, Solaris
application         : Apache
service             : TCP, HTTP
rule-id             : 11206
rev                 : 2.335
```

sensor

The IPS sensors use signatures to detect attacks. IPS sensors are made up of filters and override rules. Each filter specifies a number of signature attributes and all signatures matching all the specified attributes are included in the filter. Override rules allow you to override the settings of individual signatures.

Syntax

```
config ips sensor
  edit <sensor_str>
    get
    config filter
      edit <filter_str>
        set location {all | client | server}
        set severity {all | info low medium high critical}
        set protocol <protocol_str>
        set os {all | other windows linux bsd solaris macos}
        set application <app_str>
        set status {default | enable | disable}
        set log {default | enable | disable}
        set action {block | default | pass | reject}
        set quarantine {attacker | both | interface | none}
        get
      end
    config override
      edit <override_int>
        config exempt-ip
          edit <exempt_int>
            set dst-ip <dest_ipv4mask>
            set src-ip <source_ipv4mask>
          end
        set action {block | pass | reset}
        set log {disable | enable}
        set log-packet {disable | enable}
        set quarantine {attacker | both | interface | none}
        set status {disable | enable}
      end
    set comment <comment_str>
  end
```

Variable	Description	Default
<sensor_str>	Enter the name of an IPS sensor. For a list of the IPS sensors, enter '?' instead of an IPS sensor name. Enter a new name to create a sensor.	
get	The complete syntax of this command is: config ips sensor edit <sensor_str> get end This get command returns the following information about the sensor: • name is the name of this sensor. • comment is the comment entered for this sensor. • count-enabled is the number of enabled signatures in this IPS sensor. Disabled signatures are not included. • count-pass is the number of enabled signatures configured with the pass action. • count-block is the number of enabled signatures configured with the block action. • count-reset is the number of enabled signatures configured with the reset action. • filter lists the filters in this IPS sensor. • override lists the overrides in the IPS sensor.	
<filter_str>	Enter the name of a filter. For a list of the filters in the IPS sensor, enter '?' instead of a filter name. Enter a new name to create a filter.	
location {all | client | server}	Specify the type of system to be protected. • client selects signatures for attacks against client computers. • server selects signatures for attacks against servers. • all selects both client and server signatures.	all
severity {all | info low medium high critical}	Specify the severity level or levels. Specify all to include all severity levels.	all
protocol <protocol_str>	Specify the protocols to be examined. Enter '?' to display a list of the available protocols. All will include all protocols. Other will include all unlisted protocols.	all
os {all | other windows linux bsd solaris macos}	Specify the operating systems to be protected. All will include all operating systems. Other will include all unlisted operating systems.	all
application <app_str>	Specify the applications to be protected. Enter '?' to display a list of the available applications. All will include all applications. Other will include all unlisted applications.	all
status {default | enable | disable}	Specify the status of the signatures included in the filter. • enable will enable the filter. • disable will disable the filter. • default will enable the filter and only use the filters with a default status of enable. Filters with a default status of disable will not be used.	default
log {default | enable | disable}	Specify the logging status of the signatures included in the filter. • enable will enable logging. • disable will disable logging. • default will enable logging for only the filters with a default logging status of enable. Filters with a default logging status of disable will not be logged.	default

Variable	Description	Default
`action {block | default | pass | reject}`	Specify what action is taken with traffic in which signatures ar detected. • `block` will drop the session with the offending traffic. • `pass` will allow the traffic. • `reject` will reset the session. • `default` will either pass or drop matching traffic, depending on the default action of each signature.	`default`
`quarantine {attacker | both | interface | none}`	To prevent the attacker from continuing to attack the FortiGate unit, you can quarantine the attacker to the banned user list in one of three ways. • Enter `attacker` to block all traffic sent from the attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected. • Enter `both` to block all traffic sent from the attacker's IP address to the target (victim's) IP address. Traffic from the attacker's IP address to addresses other than the victim's IP address is allowed. The attacker's and target's IP addresses are added to the banned user list as one entry. • Enter `interface` to block all traffic from connecting to the FortiGate unit interface that received the attack. The interface is added to the banned user list. • Enter `none` to disable the adding of addresses to the quarantine but the current DoS sensor.	none

`get`	The complete syntax of this command is:
	`config ips sensor`
	`edit <sensor_str>`
	`config filter`
	`edit <filter_str>`
	`get`
	`end`
	This get command returns the following information about the filter:
	• `name` is the name of this filter.
	• `count` is the total number of signatures in this filter. Both enabled and disabled signatures are included.
	• `location` is type of system targeted by the attack. The locations are client and server.
	• `severity` is the relative importance of the signature, from info to critical.
	• `protocol` is the type of traffic to which the signature applies. Examples include HTTP, POP3, H323, and DNS.
	• `os` is the operating systems to which the signature applies.
	• `application` is the program affected by the signature.
	• `status` displays whether the signature state is enabled, disabled, or default.
	• `log` displays the logging status of the signatures included in the filter. Logging can be set to enabled, disabled, or default.
	• `action` displays what the FortiGate does with traffic containing a signature. The action can be set to pass all, block all, reset all, or default.
	• `quarantine` displays how the FortiGate unit will quarantine attackers.	

`<override_int>`	Enter the rule ID of an override filter. The rule ID is number assigned to a filter, pre-defined or custom, and it specified which filter is being overridden. For a list of the currently defined overrides, enter '?' instead of a rule ID. Rule IDs are an attribute of every signature. Use the `config ips rule` command to list the signatures or view them in the GUI.	

Variable	Description	Default
<exempt_int>	Each override can apply to any number of source addresses, destination addresses, or source/destination pairs. The addresses are referenced by exempt_id values.	
dst-ip <dest_ipv4mask>	Enter the destination IP address and subnet to which this sensor will apply. The default is all addresses.	0.0.0.0 0.0.0.0
src-ip <source_ipv4mask>	Enter the source IP address and subnet to which this sensor will apply. The default is all addresses.	0.0.0.0 0.0.0.0
action {block | pass | reset}	Specify the action to be taken for this override. • block will drop the session. • pass will allow the traffic. • reset will reset the session.	pass
log {disable | enable}	Specify whether the log should record when the override occurs.	disable
log-packet {disable | enable}	When enabled, packet logging will save the packet that triggers the override. You can download the packets in pcap format for diagnostic use. This feature is only available in FortiGate units with internal hard drives.	disable
status {disable | enable}	Enable or disable the override.	disable
comment <comment_str>	Enter a description of the IPS sensor. This description will appear in the ISP sensor list. Descriptions with spaces must be enclosed in quotes.	

Example

This example shows how to create an IPS sensor containing a filter that includes all signatures to protect against Windows server attacks.

```
config ips sensor
  edit dept_srv
    set comment "Department file servers"
    config filter
      edit win_srv
        set location server
        set os windows
        set action block
      end
  end
```

History

FortiOS v3.0 MR6 New.

FortiOS v4.0 Added the quarantine option.

log

Use the `config log` commands to set the logging type, the logging severity level, and the logging location for the FortiGate unit.

Note: In Transparent mode, certain log settings and options may not be available because certain features do not support logging or are not available in this mode. For example, SSL VPN events are not available in Transparent mode.

custom-field

Use the following command to customize the log fields with a name and/or value. The custom name and/or value will appear in the log message.

Syntax

```
config log custom-field
  edit id <integer>
    set name <name>
    set value <integer>
end
```

Variable	Description	Default
id <integer>	Enter the identification number for the log field.	No default
name <name>	Enter a name to identify the log. You can use letters, numbers, ('_'), but no characters such as the number symbol (#). The name cannot exceed 16 characters.	No default
value <integer>	Enter a firewall policy number to associate a firewall policy with the logs.	No default

Example

This example shows how to configure a customized field for logs for branch offices in a company and are associated with specific firewall policies.

```
config log custom-field
  edit 1
    set name company_branch1
    set value 2
  next
  edit 2
    set name company_branch2
    set value 4
  next
  edit 3
    set name company_branch3
    set value 5
end
```

History

FortiOS v3.0 MR6 New.

Related topics

- {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter

{disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter

Use this command to configure log filter options. Log filters define the types of log messages sent to each log location. Use the ? command to view each filter setting since not all filter settings display for each device.

Filter settings for `fortiguard` are only available when FortiGuard Analysis and Management Service is enabled. Filter settings for `disk` is available only for FortiGate units with hard disks.

Syntax

```
config log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 |memory |
   syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter
  set admin {disable | enable}
  set allowed {disable | enable}
  set anomaly {disable | enable}
  set app-crtl {disable | enable}
  set app-crtl-all {disable | enable}
  set attack {disable | enable}
  set auth {disable | enable}
  set amc-intf-bypass {disable | enable}
  set blocked {disable | enable}
  set dlp {disable | enable}
  set dlp-all {disable | enable}
  set cpu-memory-usage {disable | enable}
  set dhcp {disable | enable}
  set email {disable | enable}
  set email-log-imap {disable | enable}
  set email-log-pop3 {disable | enable}
  set email-log-smtp {disable | enable}
  set event {disable | enable}
  set ftgd-wf-block {disable | enable}
  set ftgd-wf-errors {disable | enable}
  set ha {disable | enable}
  set infected {disable | enable}
  set ipsec {disable | enable}
  set ldb-monitor {disable | enable}
  set other-traffic {disable | enable}
  set oversized {disable | enable}
  set pattern {disable | enable}
  set ppp {disable | enable}
  set scanerror {disable | enable}
  set severity {alert | critical | debug | emergency | error | information |
     notification | warning}
  set signature {disable | enable}
  set sslvpn-log-adm {disable | enable}
  set sslvpn-log-auth {disable | enable}
  set sslvpn-log-session {disable | enable}
  set system {disable | enable}
  set traffic {disable | enable}
  set url-filter {disable | enable}
  set violation {disable | enable}
  set virus {disable | enable}
```

```
    set vip-ssl {disable | enable}
    set wanopt-traffic {disable | enable}
    set wan-opt {disable | enable}
    set web {disable | enable}
    set web-content {disable | enable}
    set web-filter-activex {disable | enable}
    set web-filter-applet {disable | enable}
    set web-filter-cookie {disable | enable}
    set webcache-traffic {disable | enable}
  end
```

Variable	Description	Default
admin {disable | enable}	Enable or disable logging all administrative events, such as user logins, resets, and configuration updates in the event log. This field is available when event is enabled.	enable
allowed {disable | enable}	Enable or disable logging all traffic that is allowed according to the firewall policy settings in the traffic log. This field is available when traffic is enabled.	enable
amc-intf-bypass {disable | enable}	Enable or disable logging of the AMC interface entering by-pass mode.	enable
anomaly {disable | enable}	Enable or disable logging all detected and prevented attacks based on unknown or suspicious traffic patterns, and the action taken by the FortiGate unit in the attack log. This field is available when attack is enabled.	enable
app-crtl {disable | enable}	Enable or disable logging of application control logs.	enable
app-crtl-all {disable | enable}	Enable or disable logging of the sub-category of application control logs.	disable
attack {disable | enable}	Enable or disable the attack log.	enable
auth {disable | enable}	Enable or disable logging all firewall-related events, such as user authentication in the event log. This field is available when event is enabled.	enable
amc-intf-bypass {disable | enable}	Enable or disable logging of an AMC interface entering bypass mode messages.	enable
blocked {disable | enable}	Enable or disable logging all instances of blocked files.	enable
dlp {disable | enable}	Enable or disable logging of data leak prevention events.	enable
dlp-all {disable | enable}	Enable or disable logging of all data leak prevention subcategories.	disable
dlp-archive {disable | enable}	Enable or disable logging of data leak prevention content archive events.	enable
cpu-memory-usage {disable | enable}	Enable or disable to log CPU usage every five minutes.	disable
dhcp {disable | enable}	Enable or disable logging of DHCP service messages.	enable
email {disable | enable}	Enable or disable the spam filter log.	enable
email-log-imap {disable | enable}	Enable or disable logging of spam detected in IMAP traffic. email enable only.	enable
email-log-pop3 {disable | enable}	Enable or disable logging of spam detected in POP3 traffic. email enable only.	enable

Variable	Description	Default
email-log-smtp {disable | enable}	Enable or disable logging of spam detected in SMTP traffic. email enable only.	enable
event {disable | enable}	Enable or disable writing event log messages. This option is available only for memory and disk logs.	enable
ftgd-wf-block {disable | enable}	Enable or disable logging of web pages blocked by FortiGuard category filtering in the web filter log. This field is available when web is enabled.	enable
ftgd-wf-errors {disable | enable}	Enable or disable logging all instances of FortiGuard category filtering rating errors. This field is available when web is enabled.	enable
ha {disable | enable}	Enable or disable HA activity messages.	enable
infected {disable | enable}	Enable or disable logging of all virus infections in the antivirus log. This field is available when virus is enabled.	enable
ipsec {disable | enable}	Enable or disable logging of IPSec negotiation events, such as progress and error reports in the event log. This field is available when event is enabled.	enable
ldb-monitor {disable | enable}	Enable or disable logging of VIP realserver health monitoring messages.	disable
other-traffic {disable | enable}	Enable or disable ICSA compliant logs. This setting is independent from the traffic setting. Traffic log entries include generating traffic logs: • for all dropped ICMP packets • for all dropped invalid IP packets • for session start and on session deletion This setting is not rate limited. A large volume of invalid packets can dramatically increase the number of log entries.	disable
oversized {disable | enable}	Enable or disable logging of oversized files in the antivirus log. This field is available when virus is enabled.	enable
pattern {disable | enable}	Enable or disable logging of all pattern update events, such as antivirus and IPS pattern updates and update failures in the event log. This field is available when event is enabled.	enable
ppp {disable | enable}	Enable or disable logging of all L2TP, PPTP, and PPPoE-related events, such as manager and socket creation processes, in the event log. This field is available when event is enabled.	enable
scanerror {disable | enable}	Enable or disable logging of antivirus error messages.	enable
severity {alert | critical | debug | emergency | error | information | notification | warning}	Select the logging severity level. The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select error, the unit logs error, critical, alert and emergency level messages. emergency - The system is unusable. alert - Immediate action is required. critical - Functionality is affected. error - An erroneous condition exists and functionality is probably affected. warning - Functionality might be affected. notification - Information about normal events. information - General information about system operations. debug - Information used for diagnosing or debugging the FortiGate unit.	information
signature {disable | enable}	Enable or disable logging of detected and prevented attacks based on the attack signature, and the action taken by the FortiGate unit, in the attack log. This field is available when attack is enabled.	enable
sslvpn-log-adm {disable | enable}	Enable or disable logging of SSL-VPN administration.	enable

Variable	Description	Default
sslvpn-log-auth {disable | enable}	Enable or disable logging of SSL-VPN user authentication.	enable
sslvpn-log-session {disable | enable}	Enable or disable logging of SSL-VPN sessions.	enable
system {disable | enable}	Enable or disable logging of system activity messages.	enable
traffic {disable | enable}	Enable or disable the traffic log.	enable
url-filter {disable | enable}	Enable or disable logging of blocked URLs (specified in the URL block list) in the web filter log. This field is available when web is enabled.	enable
violation {disable | enable}	Enable or disable logging of all traffic that violates the firewall policy settings in the traffic log. This field is available when trafic is enabled.	enable
virus {disable | enable}	Enable or disable the antivirus log.	enable
vip-ssl {disable | enable}	Enable or disable logging of VIP SSL messages.	enable
wanopt-traffic {disable | enable}	Enable or disable WAN optimization traffic logging.	enable
wan-opt {disable | enable}	Enable or disable logging of wan optimization messages.	disable
web {disable | enable}	Enable or disable the web filter log.	enable
web-content {disable | enable}	Enable or disable logging of blocked content (specified in the banned words list) in the web filter log. This field is available when web is enabled.	enable
web-filter-activex {disable | enable}	Enable or disable the logging of Active X block messages.	enable
web-filter-applet {disable | enable}	Enable or disable the logging of java applet block messages.	enable
web-filter-cookie {disable | enable}	Enable or disable the logging of cookie block messages.	enable
webcache-traffic {disable | enable}	Enable or disable WAN optimization web cache traffic logging.	enable

Example

This example shows how to set the logging severity level to warning, enable virus logging for infected files, and enable event logging for anomaly and IPSec events.

```
config log disk filter
  set severity warning
  set virus enable
  set infected enable
  set event enable
  set anomaly enable
  set ipsec enable
end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v2.80 MR2	Removed `email_content` field. Added `email_log_imap`, `email_log_pop3`, and `email_log_smtp` fields.
FortiOS v3.0	`cat-monitor`, `exempt`, and `content-keywords` commands removed. `url-block` command renamed to `url-filter`. `cat-block` and `cat-errors` commands renamed to `ftgd-wf-block` and `ftgd-wf-errors` respectively. New fields `im`, `im-all` and `sslvpn-auth`, `sslvpn-adm`, `sslvpn-session`, `web-filter-activex`, `web-filter-applet` and `web-filter-cookie` added.
FortiOS v.3.0 MR4	Added the FortiGuard Log and Analysis command, `fortiguard` for configuring the filter settings for the FortiGuard Log & Analysis server. Also added VoIP commands.
FortiOS v3.0 MR7	Added `ldb-monitor` and `cpu-memory-usage` fields.
FortiOS v4.0	Added the following fields: • `app-crtl` • `app-crtl-all` • `dlp` • `dlp-all` • `wan-opt` • `amc-intf-bypass` • `content-log` • `content-log-ftp` • `content-log-http` • `content-log-imap` • `content-log-pop3` • `content-log-smtp` Removed the following fields: • `im` • `im-all` • `voip` • `voip-all`
FortiOS 4.0 MR1	Added `wanopt-traffic`, `webcache-traffic`, `scanerror`, `amc-intf-bypass`, and `dlp-archive` fields. Removed the `content-log`, `content-log-ftp`, `content-log-http`, `content-log-imap`, `content-log-pop3`, and `content-log-smtp` fields.

Related topics

- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log memory setting
- log {syslogd | syslogd2 | syslogd3} setting
- log webtrends setting
- log trafficfilter
- firewall

disk setting

Use this command to configure log settings for logging to the local disk. Disk logging is only available for FortiGate units with an internal hard disk. You can also use this command to configure the FortiGate unit to upload current log files to an FTP server every time the log files are rolled.

If you have an AMC disk installed on your FortiGate unit, you can use `disk setting` to configure logging of traffic to the AMC disk. The AMC disk behaves as a local disk after being inserted into the FortiGate unit and the FortiGate unit rebooted. You can view logs from *Log&Report* > *Log Access* > *Disk* when logging to an AMC disk.

You can also use this command to enable SQL logs for different log types. SQL logs are stored in an SQLlite database format. The main advantage of SQL log format is that it supports enhanced reports. For information about the report commands, see "report" on page 257:

Note: AMC disk is supported on all FortiGate units that have single-width AMC slots.

Syntax

```
config log disk setting
  set status {enable | disable}
  set max-log-file-size <integer  max>
  set roll-schedule {daily | weekly}
  set roll-time <hh:mm>
  set diskfull {nolog | overwrite}
  set sql-max-size <lsize>
  set sql-max-size-action {overwrite | nolog}
  set sql-oldest-entry <days>
  set upload {enable | disable}
  set upload-destination {fortianalyzer | ftp-server}
  set uploadip <class_ip>
  set uploadport <port_integer>
  set uploaduser <user_str>
  set uploadpass <passwd>
  set uploaddir <dir_name_str>
  set uploadtype {attack event im spamfilter traffic virus voip webfilter}
  set uploadzip {disable | enable}
  set uploadsched {disable | enable}
  set uploadtime <time_integer>
  set upload-delete-files {enable | disable}
  set full-first-warning threshold
  set full-second-warning threshold
  set full-final-warning threshold
  set drive-standby-time <0-19800>
  config sql-logging
    set app-ctr {disable | enable}
    set attack {disable | enable}
    set dlp {disable | enable}
    set event {disable | enable}
    set spam {disable | enable}
    set traffic {disable | enable}
    set virus {disable | enable}
    set webfilter {disable | enable}
  end
```

```
end
```

Variable	Description	Default
`status {enable | disable}`	Enter to either enable or disable logging to the local disk.	`disable`
`max-log-file-size <integer max>`	Enter the maximum size of the log file (in MB) that is saved to the local disk. When the log file reaches the specified maximum size, the FortiGate unit saves the current log file and starts a new active log file. The default minimum log file size is 1 MB and the maximum log file size allowed is 1024MB.	`100`
`roll-schedule {daily | weekly}`	Enter the frequency of log rolling. When set, the FortiGate unit will roll the log event if the maximum size has not been reached.	`daily`
`roll-time <hh:mm>`	Enter the time of day, in the format `hh:mm`, when the FortiGate unit saves the current log file and starts a new active log file.	`00:00`
`diskfull {nolog | overwrite}`	Enter the action to take when the local disk is full. When you enter `nolog`, the FortiGate unit will stop logging; `overwrite` will begin overwriting the oldest file once the local disk is full.	`overwrite`
`sql-max-size <lsize>`	Set maximum size of SQL logs. Range 1 to 65 536.	`100`
`sql-max-size-action {overwrite | nolog}`	Select action when maximum log size is reached: **`overwrite`** — Overwrite oldest logs first **`nolog`** — Discontinue logging	`overwrite`
`sql-oldest-entry <days>`	Enter number of days to keep log entries. Use 0 to keep indefinitely.	`0`
`upload {enable | disable}`	Enable or disable uploading log files to a remote directory. Enable `upload` to upload log files to an FTP server whenever a log file rolls. Use the `uploaddir`, `uploadip`, `uploadpass`, `uploadport`, and `uploaduser` fields to add this information required to connect to the FTP server and upload the log files to a specific location on the server. Use the `uploadtype` field to select the type of log files to upload. Use the `upload-delete-files` field to delete the files from the hard disk once the FortiGate unit completes the file transfer. All `upload` fields are available after enabling the upload command.	`disable`
`upload-destination {fortianalyzer | ftp-server}`	Select to upload log files directly to a FortiAnalyzer unit or to an FTP server. When you select to upload log files directly to a FortiAnalyzer unit, you can also schedule when to upload the log files, when the log file rolls, and so on.	`disable`
`uploadip <class_ip>`	Enter the IP address of the FTP server. This is required.	`0.0.0.0`
`uploadport <port_integer>`	Enter the port number used by the FTP server. The default port is 21. Port 21 is the standard FTP port.	`21`
`uploaduser <user_str>`	Enter the user account for the upload to the FTP server. This is required.	No default.
`uploadpass <passwd>`	Enter the password required to connect to the FTP server. This is required.	No default
`uploaddir <dir_name_str>`	Enter the name of the path on the FTP server where the log files will be transferred to. If you do not specify a remote directory, the log files are uploaded to the root directory of the FTP server.	No default

Variable	Description	Default
uploadtype {attack event im spamfilter traffic virus voip webfilter}	Select the log files to upload to the FTP server. You can enter one or more of the log file types separated by spaces. Use a space to separate the log file types. If you want to remove a log file type from the list or add a log file type to the list, you must retype the list with the log file type removed or added.	traffic event spamfilter virus webfilter voip im
uploadzip {disable | enable}	Enter enable to compress the log files after uploading to the FTP server. If disable is entered, the log files are uploaded to the FTP server in plain text format.	disable
uploadsched {disable | enable}	Enable log uploads at a specific time of the day. When set to disable, the FortiGate unit uploads the logs when the logs are rolled.	disable
uploadtime <time_integer>	Enter the time of day when the FortiGate unit uploads the logs. The uploadsched setting must first be set to enable.	0
upload-delete-files {enable | disable}	Enable or disable the removal of the log files once the FortiGate unit has uploaded the log file to the FTP server.	enable
full-first-warning threshold	Enter to configure the first warning before reaching the threshold. You can enter a number between 1 and 100.	75
full-second-warning threshold	Enter to configure the second warning before reaching the threshold. You can enter a number between 1 and 100.	90
full-final-warning threshold	Enter to configure the final warning before reaching the threshold. You can enter a number between 1 and 100.	95
drive-standby-time <0-19800>	Set the power management for the hard disk. Enter the number of seconds, up to 19800. If there is no hard disk activity within the defined time frame, the hard disk will spin down to conserve energy. Setting the value to 0 disables the setting.	0
config sql-logging	Enable or disable SQL logging for the following log types. Enabling a log type means the FortiGate unit saves logs to disk in SQL format and SQL reports of the data can be created.	
app-ctr {disable | enable}	Enable or disable application control SQL logs.	enable
attack {disable | enable}	Enable or disable attack SQL logs.	enable
dlp {disable | enable}	Enable or disable DLP SQL logs.	enable
event {disable | enable}	Enable or disable event SQL logs.	enable
spam {disable | enable}	Enable or disable email filter SQL logs.	enable
traffic {disable | enable}	Enable or disable traffic SQL logs.	enable
virus {disable | enable}	Enable or disable antivirus SQL logs.	enable
webfilter {disable | enable}	Enable or disable webfilter SQL logs.	enable

Example

This example shows how to enable logging to the local disk, set the action to stop logging when the disk is full, log files have a maximum size of 300MB, roll log files daily and start a new one at 1:30pm every day.

```
config log disk setting
  set status enable
  set diskfull nolog
  set max-log-file-size 300
```

```
    set roll-schedule daily
    set roll-time 01:30
  end
```

This example shows how to enable uploading the traffic log and content archive files to an FTP server. The FTP server has the IP address 172.30.120.24, the user name is ftpone, the password is ftppass1, and the directory on the FTP server is fortigate\login.

```
config log disk setting
  set upload enable
  set uploadip 172.30.120.24
  set uploaduser ftpone
  set uploadpass ftppass1
  set uploadtype traffic content
  set uploaddir fortigate\logs
end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v2.80 MR2	Removed `ftppasswd`, `ftpserver`, and `ftpuser` fields. Added `upload` field. Added `upload`, `uploaddir`, `uploadip`, `uploadpass`, `uploadport`, `uploadtype`, and `uploaduser` fields.
FortiOS v3.0	Renamed field `filesize` to `max-log-file-size`. Removed `duration` and `unit` fields. Added `upload-delete-files` command.
FortiOS v3.0 MR2	Removed `roll-day` command.
FortiOS v3.0 MR4	Additional log files new to FortiOS 3.0 MR4 were added to `uploadtype` field, `voip` and `im`.
FortiOS v3.0 MR5	Removed the field, `content`, from `uploadtype` command. Added field, `upload-destination`, for uploading log files to a FortiAnalyzer unit.
FortiOS v3.0 MR6	Added the following fields: • `full-first-warning threshold` • `full-second-warning threshold` • `full-final-warning threshold`
FortiOS 4.0 MR1	Added the following fields: `sql-max-size`, `sql-max-size-action`, `sql-oldest-entry`, `config sql-logging`, `event`, `spam`, `traffic`, `virus`, and `webfilter`.

Related topics

- log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log memory setting
- log {syslogd | syslogd2 | syslogd3} setting
- log trafficfilter
- log webtrends setting

{fortianalyzer | syslogd} override-filter

Use this command within a VDOM to override the global configuration created with the `config log {fortianalyzer | syslogd} filter` command. The filter determines which types of log messages are sent to the FortiAnalyzer unit or syslog server. For syntax and descriptions, see "{disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter" on page 235.

History

FortiOS 4.0 MR1 New

Related topics

- {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter

fortianalyzer override-setting

Use this command within a VDOM to override the global configuration created with the `config log fortianalyzer setting` command. These settings configure the connection to the FortiAnalyzer unit. For syntax and descriptions, see "{fortianalyzer | fortianalyzer2 | fortianalyzer3} setting" on page 246.

History

FortiOS 4.0 MR1 New

Related topics

- {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting

{fortianalyzer | fortianalyzer2 | fortianalyzer3} setting

Use this command to configure the FortiGate unit to send log files to a FortiAnalyzer unit.

FortiAnalyzer units are network appliances that provide integrated log collection, analysis tools and data storage. Detailed log reports provide historical as well as current analysis of network and email activity to help identify security issues and reduce network misuse and abuse.

Using the CLI, you can send logs to up to three different FortiAnalyzer units for maximum fail-over protection of log data. After configuring logging to FortiAnalyzer units, the FortiGate unit will send the same log packets to all configured FortiAnalyzer units. Additional FortiAnalyzer units are configured using the `fortianalyzer 2` and `fortianalyzer 3` commands.

Note: The FortiAnalyzer CLI commands are not cumulative. Using a syntax similar to the following is not valid:

```
config log fortianalyzer fortianalyzer2 fortianalyzer3 setting
```

Syntax

```
config log {fortianalyzer |fortianalyzer2 | fortianalyzer3} setting
  set address-mode {auto-discovery | static}
  set conn-timeout <seconds>
  set encrypt {enable | disable}
  set fdp-device <serial_number>
  set localid <identifier>
  set max-buffer-size <size_int>
  set psksecret <pre-shared_key>
  set server <fortianalyzer_ipv4>
  set status {enable | disable}
end
```

Variable	Description	Default
`address-mode {auto-discovery | static}`	Select `auto-discovery` to automatically detect a FortiAnalyzer unit. Select `static` to enter the IP address of the FortiAnalyzer unit. Not available for `fortianalyzer2` and `fortianalyzer3`.	`static`
`conn-timeout <seconds>`	Enter the number of seconds before the FortiAnalyzer connection times out.	`10`
`encrypt {enable | disable}`	Enable to use IPSec VPN tunnel for communication. Disable to send data as plain text.	`disable`
`fdp-device <serial_number>`	Enter the serial number of the Fortianalyzer unit to connect to. This field is only available when `address-mode` is set to `auto-discovery`. Not available for `fortianalyzer2` and `fortianalyzer3`.	No default
`fdp-interface <int_str>`	Enter the interface on which the FortiGate unit will automatically detect FortiAnalyzer units.	No default
`localid <identifier>`	Enter an identifier up to 64 characters long. You must use the same identifier on the FortiGate unit and the FortiAnalyzer unit.	No default.
`max-buffer-size <size_int>`	Enter a number between 1 and 1024MB for the maximum buffer size for the FortiAnalyzer unit. The number 0 disables the maximum buffer size. This option is available for FortiGate units with hard disks.	`1`
`psksecret <pre-shared_key>`	Enter the pre-shared key for the IPSec VPN tunnel. This is needed only if `encrypt` is set to `enable`.	No default.

Variable	Description	Default
server <fortianalyzer_ipv4>	Enter the IP address of the FortiAnalyzer unit. This field is only available when address-mode is set to static.	0.0.0.0
status {enable | disable}	Enable or disable communication with the FortiAnalyzer unit. The other fields are available only if status is set to enable.	disable

Example

This example shows how to enable logging to a second FortiAnalyzer unit with IP address 192.168.20.10.

```
config log fortianalyzer2 setting
  set status enable
  set server 192.168.20.10
end
```

History

FortiOS v2.80	New.
FortiOS v2.80 MR2	Added localid and pksecret fields.
FortiOS v3.0	Moved all FortiAnalyzer configuration fields under config system fortianalyzer. Command includes up to three FortiAnalyzer units, fortianalyzer2 and fortianalyzer3. Changed FortiLog product name to FortiAnalyzer.
FortiOS v3.0 MR4	Added multi-report field.
FortiOS v3.0 MR7	Removed multi-report field.
FortiOS 4.0 MR1	The fields of config system fortianalyzer moved to this command. The config system fortianalyzer command removed from the CLI. The following fields have been added: address-mode, conn-timeout, encrypt, fdp-device, localid, psksecret, and server. The ver-1 field that was formerly part of the config system fortianalyzer command has been removed.

Related topics

- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log memory setting
- log {syslogd | syslogd2 | syslogd3} setting
- log webtrends setting
- log trafficfilter

fortiguard setting

Use this command for configuring FortiGuard Analysis Service settings. For more information about logging to a FortiGuard Analysis server, (including the subscription-based service), FortiGuard Analysis and Management Service, see the *FortiGate Administration Guide* Service, including enabling logging to a FortiGuard Analysis server.

Note: The `fortiguard setting` command is only available when FortiGuard Analysis and Management Service subscription-based services are enabled. The storage space is a specified amount, and varies, depending on the services requested.

Syntax

```
config log fortiguard setting
  set quotafull {nolog | overwrite}
  set status {disable | enable}
end
```

Variable	Description	Default
`quotafull {nolog | overwrite}`	Enter the action to take when the specified storage space on the FortiGuard Analysis server is full. When you enter `nolog`, the FortiGate unit will stop logging, and `overwrite` will begin overwriting the oldest file.	`overwrite`
`status {disable | enable}`	Enable or disable the FortiGuard Analysis service.	`disable`

Example

In this example, the FortiGate unit is logging to a FortiGuard Analysis server, and will stop logging when the maximum storage space on the server is reached.

```
config log fortiguard setting
  set quotafull nolog
  set status enable
end
```

History

FortiOS v3.0 MR4 New.

Related topics

- {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter

memory setting

Use this command to configure log settings for logging to the FortiGate system memory.

The FortiGate system memory has a limited capacity and only displays the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the FortiGate unit begins to overwrite the oldest messages. All log entries are deleted when the FortiGate unit restarts.

Syntax

```
config log memory setting
  set diskfull {overwrite}
  set status {disable | enable}
end
```

Variable	Description	Default
`diskfull {overwrite}`	Enter the action to take when the memory is reaching its capacity. The only option available is `overwrite`, which means that the FortiGate unit will begin overwriting the oldest file.	`overwrite`
`status {disable | enable}`	Enter `enable` to enable logging to the FortiGate system memory.	`disable`

Example

This example shows how to enable logging to the FortiGate system memory.

```
config log memory setting
  set status enable
  set diskfull overwrite
end
```

History

FortiOS 2.80	Substantially revised.
FortiOS v3.0	Added `diskfull` field.
FortiOS v3.0 MR6	Removed `blocktraffic` and `nolog` fields.

Related topics

- log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log {syslogd | syslogd2 | syslogd3} setting
- log webtrends setting
- log trafficfilter
- memory global-setting

memory global-setting

Use this command to configure log threshold warnings, as well as the maximum buffer lines, for the FortiGate system memory.

The FortiGate system memory has a limited capacity and displays only the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the FortiGate unit begins to overwrite the oldest log messages. All log entries are deleted when the FortiGate unit restarts.

Syntax

```
config log memory global-setting
  set full-final-warning-threshold
  set full-first-warning-threshold
  set full-second-warning-threshold
  set max-size <int>
end
```

Variable	Description	Default
full-final-warning-threshold	Enter to configure the final warning before reaching the threshold. You can enter a number between 3 and 100.	95
full-first-warning-threshold	Enter to configure the first warning before reaching the threshold. You can enter a number between 1 and 98.	75
full-second-warning-threshold	Enter to configure the second warning before reaching the threshold. You can enter a number between 2 and 99.	90
max-size <int>	Enter the maximum size of the memory buffer log, in bytes.	98304

Example

This example shows how to configure the first, second, and final threshold warnings as well as the maximum lines for the memory buffer log.

```
config log memory global setting
  set first-full-warning-threshold 40
  set second-full-warning-threshold 60
  set final-full-warning-threshold 80
  set max-size 98304
end
```

History

FortiOS v3.0 MR6 New.

FortiOS v4.0 MR1 `max-lines` command changed to `max-size`.

Related topics

- log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log {syslogd | syslogd2 | syslogd3} setting
- log webtrends setting
- log trafficfilter
- memory setting

syslogd override-setting

Use this command within a VDOM to override the global configuration created with the `config log syslogd setting` command. These settings configure the connection to a syslog server. For syntax and descriptions, see "{syslogd | syslogd2 | syslogd3} setting" on page 252.

History

FortiOS 4.0 MR1 New

Related topics

- {syslogd | syslogd2 | syslogd3} setting

{syslogd | syslogd2 | syslogd3} setting

Use this command to configure log settings for logging to a remote syslog server. You can configure the FortiGate unit to send logs to a remote computer running a syslog server.

Using the CLI, you can send logs to up to three different syslog servers. Configure additional syslog servers using `syslogd2` and `syslogd3` commands and the same fields outlined below.

Note: Syslog CLI commands are not cumulative. Using a syntax similar to the following is not valid:

```
config log syslogd syslogd2 syslogd3 setting
```

Syntax

```
config log {syslogd | syslogd2 | syslogd3} setting
  set csv {disable | enable}
  set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp
     | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6
     | local7 | lpr | mail | news | ntp | syslog | user | uucp}
  set port <port_integer>
  set reliable {disable | enable}
  set server <address_ipv4>
  set status {disable | enable}
end
```

Variable	Description	Default
`csv {disable | enable}`	Enter `enable` to enable the FortiGate unit to produce the log in Comma Separated Value (CSV) format. If you do not enable CSV format the FortiGate unit produces plain text files.	`disable`
`facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}`	Enter the facility type. `facility` identifies the source of the log message to syslog. You might want to change `facility` to distinguish log messages from different FortiGate units. Available facility types are: • `alert`: log alert • `audit`: log audit • `auth`: security/authorization messages • `authpriv`: security/authorization messages (private) • `clock`: clock daemon • `cron`: cron daemon performing scheduled commands • `daemon`: system daemons running background system processes • `ftp`: File Transfer Protocol (FTP) daemon • `kernel`: kernel messages • `local0` – `local7`: reserved for local use • `lpr`: line printer subsystem • `mail`: email system • `news`: network news subsystem • `ntp`: Network Time Protocol (NTP) daemon • `syslog`: messages generated internally by the syslog daemon	`local7`
`port <port_integer>`	Enter the port number for communication with the syslog server.	`514`
`reliable {disable | enable}`	Enable reliable delivery of syslog messages to the syslog server. When enabled, the FortiGate unit implements the RAW profile of RFC 3195 for reliable delivery of log messages to the syslog server. Reliable syslog protects log information through authentication and data encryption and ensures that the log messages are reliably delivered in the correct order.	`disable`

Variable	Description	Default
`server <address_ipv4>`	Enter the IP address of the syslog server that stores the logs.	No default.
`status {disable | enable}`	Enter `enable` to enable logging to a remote syslog server.	`disable`

Example

This example shows how to enable logging to a remote syslog server, configure an IP address and port for the server, and enable logging in CSV format.

```
config log syslogd setting
  set status enable
  set server 192.168.201.199
  set port 601
  set csv enable
end
```

History

FortiOS v2.80	Substantially revised.
FortiOS 2.80 MR3	Added `alert` and `audit` fields for use with `facility` field.
FortiOS v3.0	Command includes up to three syslog servers, `syslogd2` and `syslogd3`.
FortiOS 4.0 MR1	Added `reliable` field.

Related topics

- log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log memory setting
- log webtrends setting
- log trafficfilter

webtrends setting

Use this command to configure log settings for logging to a remote computer running a NetIQ WebTrends firewall reporting server.

FortiGate log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with NetIQ WebTrends Security Reporting Center and Firewall Suite 4.1.

Syntax

```
config log webtrends setting
  set server <address_ipv4>
  set status {disable | enable}
end
```

Variable	Description	Default
`server <address_ipv4>`	Enter the IP address of the WebTrends server that stores the logs.	No default.
`status {disable | enable}`	Enter `enable` to enable logging to a WebTrends server.	`disable`

Example

This example shows how to enable logging to and set an IP address for a remote WebTrends server.

```
config log webtrends setting
  set status enable
  set server 192.168.21.155
end
```

History

FortiOS v2.80 Substantially revised.

Related topics

- log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log memory setting
- log {syslogd | syslogd2 | syslogd3} setting
- log trafficfilter

trafficfilter

Use this command to configure the following global settings for traffic logging:

- resolve IP addresses to host names
- display the port number or service (protocol) in the log message

Syntax

```
config log trafficfilter
  set display {name | port}
  set resolve {disable | enable}
end
```

Variable	Description	Default
`display {name | port}`	Enter `name` to enable the display of the service name in the traffic log messages. Enter `port` to display the port number used by traffic in traffic log messages.	`port`
`resolve {disable | enable}`	Enter `enable` to enable resolving IP addresses to host names in traffic log messages.	`disable`

Example

This example shows how to display the service name and enable resolving IP addresses to host names in log messages.

```
config log trafficfilter
  set display name
  set resolve enable
end
```

History

FortiOS v2.80 Revised.

FortiOS v3.0 MR7 Removed the `config rule` sub-command.

Related topics

- log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- log memory setting
- log {syslogd | syslogd2 | syslogd3} setting
- log webtrends setting

report

Use the `config report` commands to configure executive summary SQL widgets. Using these commands you can edit existing widgets and create new widgets.

All of these widgets are available from the FortiGate web-based manager by going to *Log&Report* > *Report Access* > *Executive Summary*. Select *Add Widget* to add widgets to the *Executive Summary*. Three report commands are available:

- Use the `config report dataset` command to configure datasets. A dataset consists of SQL statements that query the SQL log database and gather data. The SQL statement must include references to the SQL database containing the log message data. For information about the SQL database format, see "SQL reports database schema" on page 268.
- Use the `config report chart` command to configure charts that can be added to the Executive Summary. A chart, called a Widget when you add it to the *Executive Summary* page, includes a dataset that queries the SQL database and settings that configure l how the data gathered by the dataset is displayed by the widget. For example, you can use the `config report chart` command to set the title, the graph type, and the scale and appearance of the x and y axis of the widget.
- Use the `config report summary` command to add widgets to the Executive Summary and to configure the schedule for how often the data displayed by the widget is refreshed. This data is refreshed by running the SQL query in the widget.

chart

Use the following command to configure a chart or widget. You can edit the settings of existing widgets or you can add new widgets. To add a new widget you need to have a dataset for it as well as a title. You can also configure the widget to be a graph in various formats or a table and you can also optionally configure details about the appearance of the graph or table.

As you change chart format settings you can go to the Executive Summary page of the web-based manager and view the chart. Refresh your browser to see format changes. You must use the `end` command to exit from the `config report chart` command to view your changes in the widget.

Tip: Charts are called widgets in the Executive Summary on the web-based manager. In the web-based manager each widget has a name which is set using the `comments` field of the `config report chart` command. When you edit a chart you specify a chart name that is only used in the CLI. To determine the widget name of a chart you must edit it and view the `comments` setting.

Syntax

Note: Due to the complexity and duplication in the `chart` command, the `set` commands are listed in simple alphabetical order.

```
config report chart
  edit <chart_name>
      config category-series
      config column
        edit <column_number>
            config mapping
              edit <id>
      config value-series
      config x-series
      config y-series
      end
    set background <color_hex>
    set caption <caption_str>
    set caption-font-size <size_int>
    set color-palette <palette_hex>
    set comments <comment_str>
    set databind <value_expr_str>
    set dataset <dataset_name>
    set detail-unit <unit_str>
    set detail-value <value-str>
    set dimension {2D | 3D}
    set displayname <name_str>
    set extra-databind <value_expr_str>
    set extra-y {disable |enable)
    set extra-y-legend <legend_string>
    set footer-unit <string>
    set footer-value <value-str>
    set font-size <size_int>
    set graph-type {bar | flow | line | none | pie}
    set group <group_str>
    set header-value <string>
    set is-category {no | yes}
    set label-angle {45-degree | vertical | horizontal}
```

```
set legend {enable | disable}
set legend-font-size <size_int>
set op {equal | greater | greater-equal | less | less-equal | none}
set scale-format {YYYY-MM-DD-HH-MM | YYYY-MM-DD | HH | YYYY-MM-DD |
   YYYY-MM | YYYY | HH-MM | MM-DD}
set scale-number-of-step <steps_int>
set scale-origin {max | min}
set scale-start {now | hh:mm yyyy/mm/dd}
set scale-step <step_int>
set scale-type datetime
set scale-unit {day | hour | minute | month | year}
set style {auto | manual}
set title <title_str>
set title-font-size <size_int>
set type {graph | table}
set unit <unit_str>
set value1 {<value_int> | <value_str>}
set value2 {<value_int> | <value_str>}
set value-type {integer | string}
set y-legend <legend_str>
end
```

Variable	Description	Default
`config category-series`	Configure the category settings required for a pie chart.	
`config column`	Configure columns for a table. To configure these settings `style` must be `manual` and `type` must be `table`. You can add multiple columns to the table and configure settings for each column.	
`config mapping`	Configure mapping for a table.	
`config value-series`	Configure the value settings required for a pie chart.	
`config x-series`	Configure settings for the x axis of a bar or line graph. To configure these settings `style` must be `manual` and `type` must be `graph`.	
`config y-series`	Configure settings for the y axis of a bar or line graph. To configure these settings `style` must be `manual` and `type` must be `graph`.	
`<chart_name>`	Enter the name of a new or existing chart. The `<chart_name>` only appears in the CLI. The web-based manager includes widget names that are set using the `comments` field.	
`<column_number>`	Enter the number of the column to configure. Columns are numbered from the left starting at 1.	
`<id>`	Identifies a mapping instance.	
`background <color_hex>`	Enter the hexidecimal value for an HTML color to set the background color for a graph. The color value should begin with `0x`. For example, the color `0xff0000` results in a red background.	
`caption <caption_str>`	Add a caption text string.	
`caption-font-size <size_int>`	Set the size of the font used to display a caption. 0 means the font size is set automatically. The font size range is 5 to 20.	`0`
`color-palette <palette_hex>`	Enter the hexidecimal value for an HTML color palette. The color palette value should begin with `0x`.	
`comments <comment_str>`	Enter the name of the widget. You use this name to select the widget when adding it to the Executive Summary from the web-based manager. This name appears at the top of the widget when it is displayed in the Executive Summary.	No default.
`databind <value_expr_str>`	Enter an SQL databind value expression for binding data to the series being configured.	

Variable	Description	Default
dataset <dataset_name>	Enter the name of the dataset that provides the data for this chart. Use the config report dataset command to add or edit data sets. The default configuration includes a number of pre-configured data sets.	No default.
detail-unit <unit_str>	Enter an abbreviation to display for the measurement unit, “MB”, for example.	
detail-value <value-str>	Define the value to appear in each column of a table.	
dimension {2D | 3D}	Define whether bar and pie graphs will have a 2D or 3D display.	3D
displayname <name_str>	Set the name to be displayed for a mapping.	
extra-databind <value_expr_str>	Enter an SQL databind value expression for binding extra data to the series being configured.	
extra-y {disable |enable)	Enable or disable adding a second or extra set of data to the y-axis of a graph.	disable
extra-y-legend <legend_string>	Add a name to a second or extra set of data added to the y-axis of a graph.	
font-size <size_int>	Set the size of the font used to display a title. 0 means the font size is set automatically. The font size range is 5 to 20.	0
footer-unit <string>	Enter an abbreviation to display for the footer unit, “MB”, for example.	
footer-value <value-str>	Define the value to appear in the footer of a table.	
graph-type {bar | flow | line | none | pie}	If type is set to graph select the type of graph used to display information in the widget.	none
group <group_str>	Enter a group string.	
header-value <string>	Define the value to appear in the header of a table.	
is-category {no | yes}	Specify whether an x axis of a graph displays categories or a series of values.	no
label-angle {45-degree | vertical | horizontal}	Select the angle for displaying the x or y axis label.	Varies depending on the chart and series.
legend {enable | disable}	Enable or disable the generation and display of a data legend.	enable
legend-font-size <size_int>	Set the size of the font used to display a legend. 0 means the font size is set automatically. The font size range is 5 to 20.	0
op {equal | greater | greater-equal | less | less-equal | none}	Set the mapping option	none
scale-format {YYYY-MM-DD-HH-MM | YYYY-MM-DD | HH | YYYY-MM-DD | YYYY-MM | YYYY | HH-MM | MM-DD}	Set the format for displaying the date and time on the x-axis of a graph.	YYYY-MM-DD-HH-MM
scale-number-of-step <steps_int>	Set the number of steps on the horizontal axis of the graph. The range is 1 to 31.	0

Variable	Description	Default
scale-origin {max | min}	Set the time start point and direction of time on the x-axis of the graph: • max along the x-axis time is displayed in reverse starting at the origin of the graph with the scale-start time. • min along the x-axis time is displayed in the forward direction starting at the origin of the graph with the scale-start time.	max
scale-start {now | hh:mm yyyy/mm/dd}	Set the start time for the x-axis. now sets the start time to the time that the graph was generated. You can also specify a time and date. The year range is 2001-2050.	now
scale-step <step_int>	The number of scale-units in each x-axis scale step.	0
scale-type datetime	Only the datetime scale type is supported. Sets the x-axis to display dates and times.	datetime
scale-unit {day | hour | minute | month | year}	The units of the scale-step on the x-axis.	day
style {auto | manual}	By default style is set to auto which means the appearance of the graph or chart in the widget is configured automatically. You can set style to manual to manually configure details about the appearance of the chart or graph in the widget.	auto
title <title_str>	Enter the title of the graph or table. The title is optional and appears inside the widget above the graph or chart. This is not the name of the widget. Use the comments field to add the title or name of the widget.	No default.
title-font-size <size_int>	Set the size of the font used to display the title. 0 means the font size is set automatically. The font size range is 5 to 20.	0
type {graph | table}	Configure whether this widget presents information in a graphical form as a graph or as a table of values. If you select graph use the graph-type field to configure the type of graph.	graph
unit <unit_str>	Enter the name of the units to be displayed on the x-axis.	
value-type {integer | string}	Configure the mapping value to be an integer or a text string.	integer
value1 {<value_int> | <value_str>}	Set the first mapping value.	
value2 {<value_int> | <value_str>}	Set a second mapping value if required.	
y-legend <legend_str>	Add a name for the data included on the y-axis of a graph.	

History

FortiOS v4.0 MR1 New.

Related topics

- dataset
- summary

dataset

Use the following command to configure report data sets. You can configure existing data sets or add new ones.

Note: Expert knowledge of SQL is required to write and edit data set queries.

Syntax

```
config report dataset
    edit <report_dataset>
    set query <SQL_statement>
    config field
      edit <field-id>
        set displayname <string>
        set type {text | integer | date | ip}
      next
      end
  end
```

Variable	Description	Default
`edit <report_dataset>`	Enter the name of an existing dataset or a new name. Press ? to view the list of existing datasets.	
`query <SQL_statement>`	Enter the SQL statement that retrieves the required data from the database. Comprehensive knowledge of SQL queries is required. See the existing datasets for example SQL queries.	No default.
`config field`	You should configure fields only to modify the type or displayed name of the column for use in a table or chart.	
`edit <field-id>`	Enter a field id from 1 to the number of SQL result fields in the SQL query.	
`displayname <string>`	Enter the name for the field to be displayed in tables and charts.	
`type {text | integer | date | ip}`	Select the type of data in the field. All options are not available for all fields.	`text`

History

FortiOS 4.0 MR1 New.

Related topics

- chart
- summary

summary

Use this command to add widgets (also called charts) to the Executive Summary and to configure the schedule for updating the data displayed by the widget. The data is updated by executing the SQL query in the widget and refreshing the information displayed in the widget.

Syntax

```
config report summary
  edit id <integer>
    set column {1 | 2}
    set day {sunday | monday | tuesday | wednesday | thursday | friday |
       saturday}
    set schedule {daily | weekly}
    set time <hh:mm>
    set widget <widget_name>
end
```

Variable	Description	Default
`id <integer>`	Enter the identification number for the log field.	No default
`column {1 | 2}`	Select the column of the Executive Summary to display the widget in.	`1`
`day {sunday | monday | tuesday | wednesday | thursday | friday | saturday}`	Set the day of the week to update the widget. Available if `schedule` is `weekly`.	`sunday`
`schedule {daily | weekly}`	Schedule the widget to update once a day or once a week.	`daily`
`time <hh:mm>`	Set the time of day to update the widget. You can set the time of day for weekly or daily updates.	`00:00`
`widget <widget_name>`	Select the name of the widget.	

History

FortiOS v4.0 MR1 New.

Related topics

- chart
- summary

Example SQL report configurations

Example WAN optimization SQL report configuration

The following is an example configuration for WAN optimization reports based on SQL logs using a bar chart.

```
config report chart
  edit "wanopt-bw-per-app-last24h"
    set dataset "wanopt-bandwidth-per-app-last24h"
    set graph-type bar
      config x-series
        set databind "field(1)"
      end
      config y-series
        set databind "field(3)"
        set extra-databind "field(2)"
        set extra-y enable
        set extra-y-legend "LAN"
        set y-legend "WAN"
      end
    set title "per apptype wanopt bandwidth summary"
  next
  edit "wanopt-lan-bw-per-app-last24h"
    set dataset "wanopt-lan-bw-per-app-last24h"
    set graph-type pie
    set style manual
      config category-series
        set databind "field(1)"
      end
      config value-series
        set databind "field(3)"
      end
    set title "Wanopt Lan Bandwidth"
  next
  edit "wanopt-bw-per-hour-last24h-tbl"
    set type table
    set dataset "wanopt-bandwidth-per-hour-last24h"
      config column
        edit 1
          set detail-value "ctime(\'DD HH-MM\', field(1))"
          set header-value "Time"
        next
        edit 2
          set detail-value "field(2)+\' MB\'"
          set header-value "LAN"
        next
        edit 3
          set detail-value "field(3)+\' MB\'"
          set header-value "WAN"
        next
        edit 4
          set detail-value "field(4)+\'%\'"
          set header-value "Reduction Rate"
        next
```

```
        end
    next
    end

    config report dataset
      edit "wanopt-bandwidth-per-hour-last24h"
        set query "select (timestamp-timestamp%3600) as
           hourstamp,sum(lan_in+lan_out) / 1000000.0 as lan, sum(wan_in+wan_out)
           / 1000000.0 as wan,max(coalesce((sum(lan_in+lan_out)-
           sum(wan_in+wan_out))*100.0/sum(lan_in+lan_out),0.0), 0.0) as
           reduce_rate from traffic_log where timestamp
           >=F_TIMESTAMP(\'now\',\'hour\',\'-23\') and subtype=\'wanopt-
           traffic\' group by hourstamp order by hourstamp desc"
      next
      edit "wanopt-bandwidth-per-app-last24h"
        set query "select (case (wanopt_app_type in ( select wanopt_app_type
           from traffic_log where subtype=\'wanopt-traffic\' and timestamp >=
           F_TIMESTAMP(\'now\',\'hour\',\'-23\') group by wanopt_app_type order
           by sum(lan_in+lan_out) desc limit 5) ) when 1 then wanopt_app_type
           else \'others\' end) as wanopt_app_type,
           sum(lan_in+lan_out)/1000000.0 as lan,sum(wan_in+wan_out)/1000000.0
           as wan,max(coalesce((sum(lan_in+lan_out)-
           sum(wan_in+wan_out))*100.0/sum(lan_in+lan_out),0.0), 0.0) as
           reduce_rate from traffic_log where subtype=\'wanopt-traffic\' and
           timestamp >=F_TIMESTAMP(\'now\',\'hour\',\'-23\') group by
           wanopt_app_type order by lan desc"
      next
      edit "wanopt-lan-bw-per-app-last24h"
        set query "select (case (wanopt_app_type in ( select wanopt_app_type
           from traffic_log where subtype=\'wanopt-traffic\' and timestamp >=
           F_TIMESTAMP(\'now\',\'hour\',\'-23\') group by wanopt_app_type order
           by sum(lan_in+lan_out) desc limit 5) ) when 1 then wanopt_app_type
           else \'others\' end) as wanopt_app_type,
           sum(lan_in+lan_out)/1000000.0 as
           lan,max(coalesce((sum(lan_in+lan_out)*100.0/(select
           sum(lan_in+lan_out) from traffic_log where subtype=\'wanopt-traffic\'
           and timestamp >= F_TIMESTAMP(\'now\',\'hour\',\'-23\'))),0.0),0.0) as
           percentage from traffic_log where subtype=\'wanopt-traffic\' and
           timestamp >=F_TIMESTAMP(\'now\',\'hour\',\'-23\') group by
           wanopt_app_type order by lan desc"
      next
end
```

Example attack SQL report configuration

The displaying the number of attacks per hour for the last 24 hours using a bar chart.

```
config report dataset
  edit "attackcount-per-hour-last24h"
    set query "select (timestamp-timestamp%3600) as hourstamp, severity,
       count(*)  from attack_log where timestamp >=
       F_TIMESTAMP(\'now\',\'hour\',\'-23\') group by hourstamp, severity
       order by hourstamp desc"
      config field
       edit 1
         set type integer
       next
       end
    next
    edit "top-app-last24h"
      set query "select app, count(*) as totalnum from app_control_log where
         timestamp >= F_TIMESTAMP(\'now\',\'hour\',\'-23\') group by app
         order by totalnum desc limit 20"
    next
    edit "latest-attack"
      set query "select attack_id, timestamp, severity, src, dst, src_port,
         dst_port, proto, service, user, usergroup, app_list from attack_log
         order by timestamp desc limit 100"
    next

end
  config report chart
    edit "attackcount-per-hour-last24h"
      set comments "stacked bar"
      set dataset "attackcount-per-hour-last24h"
      set graph-type bar
        config x-series
          set databind "field(1)"
          set is-category no
          set scale-format HH:MM
          set scale-number-of-step 24
          set scale-step 1
          set scale-unit hour
        end
        config y-series
          set databind "field(3)"
          set group "field(2)"
        end
      set title "Per Hour Attack Summary"
    next
    edit "top-app-last24h"
      set dataset "top-app-last24h"
      set graph-type bar
        config x-series
          set databind "field(1)"
        end
        config y-series
          set databind "field(2)"
```

```
    end
  set title "Top 20 Application"
next
edit "latest-attack-last24h"
  set type table
  set dataset "latest-attack-last24h"
    config column
      edit 1
        set detail-value "attack_id2name(field(1))"
        set header-value "Attack ID"
      next
      edit 2
        set detail-value "ctime(\'YYYY/MM/DD HH:MM\', field(2))"
        set header-value "Timestamp"
      next
      edit 3
        set detail-value "field(4)"
        set header-value "Source"
      next
      edit 4
        set detail-value "field(5)"
        set header-value "Destination"
      next
      edit 5
        set detail-value "field(3)"
        set header-value "Severity"
      next
      end
end
```

SQL reports database schema

This section lists the fields in the SQL database for each log message type. The SQL database follows the SQLite 3.0 database schema. Please note the following:

- `oid`, is primary key that identifies the event and log message.
- `timestamp` is stored as `ctime`, but as an integer type for easier sorting and searching.
- `timeperiod` is 15 minutes and is accomplished by grouping log messages every 15 30 minutes.
- `other` fields are general fields in the original raw log.
- all IPv4 and IPv6 addresses are stored as integers.

You can use the command `get report database schema` to list all of the tables and fields in the SQL log database.

Event Log

```
CREATE TABLE event_log
(
      "oid"                     INTEGER PRIMARY KEY AUTOINCREMENT,
      "timestamp"               INTEGER,
      "log_id"                  INTEGER,
      "subtype"                 TEXT,
      "pri"                     TEXT,
      "extra"                   TEXT,
      "user"                    TEXT,
      "ui"                      TEXT,
      "action"                  TEXT,
      "status"                  TEXT,
      "reason"                  TEXT,
      "cpu"                     INTEGER,
      "mem"                     INTEGER,
      "total_session"           INTEGER,
      "obj"                     TEXT,
      "entry"                   TEXT,
      "field"                   TEXT,
      "old_value"               TEXT,
      "new_value"               TEXT,
      "acct_stat"               TEXT,
      "count"                   INTEGER,
      "duration"                TEXT,
      "carrier_ep"              TEXT,
      "from"                    TEXT,
      "ip"                      TEXT,
      "nf_type"                 TEXT,
      "profile"                 TEXT,
      "proto"                   INTEGER,
      "service"                 TEXT,
      "to"                      TEXT,
      "tunnel_id"               INTEGER,
      "tunnel"                  TEXT,
      "tunnel_type"             TEXT,
      "tunnel_action"           TEXT,
      "remote_ip"               TEXT,
      "tunnel_ip"               TEXT,
```

```
        "vpn_user"              TEXT,
        "vpn_usergroup"         TEXT,
        "xauth_user"            TEXT,
        "xauth_group"           TEXT,
        "dst_host"              TEXT,
        "next_stats"            INTEGER,
        "vpn_duration"          INTEGER,
        "sent"                  INTEGER,
        "rcvd"                  INTEGER,
        "vpn_reason"            TEXT,
        "alert"                 TEXT,
        "desc"                  TEXT,
        "app_type"              TEXT,
        "msg"                   TEXT,
        "ha_role"               TEXT,
        "vcluster_state"        TEXT,
        "hbdn_reason"           TEXT,
        "ha_group"              INTEGER,
        "vcluster"              INTEGER,
        "from_vcluster"         INTEGER,
        "to_vcluster"           INTEGER,
        "vcluster_member"       INTEGER,
        "vdname"                TEXT,
        "devintfname"           TEXT,
        "hostname"              TEXT,
        "sn"                    TEXT
)
```

Traffic log

```
CREATE TABLE traffic_log
(
        "oid"                   INTEGER PRIMARY KEY AUTOINCREMENT,
        "timestamp"             INTEGER,
        "log_id"                INTEGER,
        "subtype"               TEXT,
        "pri"                   TEXT,
        "dir_disp"              TEXT,
        "tran_disp"             TEXT,
        "src"                   TEXT,
        "srcname"               TEXT,
        "src_port"              INTEGER,
        "dst"                   TEXT,
        "dstname"               TEXT,
        "dst_port"              INTEGER,
        "tran_ip"               TEXT,
        "tran_port"             INTEGER,
        "service"               TEXT,
        "proto"                 INTEGER,
        "app_type"              TEXT,
        "duration"              INTEGER,
        "rule"                  INTEGER,
        "policyid"              INTEGER,
        "sent"                  INTEGER,
```

```
        "rcvd"                  INTEGER,
        "sent_pkt"              INTEGER,
        "rcvd_pkt"              INTEGER,
        "vpn"                   TEXT,
        "src_int"               TEXT,
        "dst_int"               TEXT,
        "SN"                    INTEGER,
        "status"                TEXT,
        "user"                  TEXT,
        "group"                 TEXT,
        "carrier_ep"            TEXT,
        "wanopt_app_type"       TEXT,
        "wan_in"                INTEGER,
        "wan_out"               INTEGER,
        "lan_in"                INTEGER,
        "lan_out"               INTEGER
)
```

Attack log

```
CREATE TABLE attack_log
(
        "oid"                   INTEGER PRIMARY KEY AUTOINCREMENT,
        "timestamp"             INTEGER,
        "log_id"                INTEGER,
        "subtype"               TEXT,
        "pri"                   TEXT,
        "policyid"              INTEGER,
        "serial"                INTEGER,
        "attack_id"             INTEGER,
        "severity"              TEXT,
        "carrier_ep"            TEXT,
        "profile"               TEXT,
        "sensor"                TEXT,
        "src"                   TEXT,
        "dst"                   TEXT,
        "src_port"              INTEGER,
        "icmp_id"               TEXT,
        "dst_port"              INTEGER,
        "icmp_type"             TEXT,
        "icmp_code"             TEXT,
        "src_int"               TEXT,
        "dst_int"               TEXT,
        "status"                TEXT,
        "proto"                 INTEGER,
        "service"               TEXT,
        "user"                  TEXT,
        "group"                 TEXT,
        "ref"                   TEXT,
        "count"                 INTEGER,
        "incident_serialno"     INTEGER,
        "msg"                   TEXT
)
```

Antivirus log

```
CREATE TABLE antivirus_log
(
      "oid"                     INTEGER PRIMARY KEY AUTOINCREMENT,
      "timestamp"               INTEGER,
      "log_id"                  INTEGER,
      "subtype"                 TEXT,
      "pri"                     TEXT,
      "msg"                     TEXT,
      "status"                  TEXT,
      "service"                 TEXT,
      "src"                     TEXT,
      "dst"                     TEXT,
      "sport"                   INTEGER,
      "dport"                   INTEGER,
      "src_int"                 TEXT,
      "dst_int"                 TEXT,
      "policyid"                INTEGER,
      "serial"                  INTEGER,
      "dir"                     TEXT,
      "filefilter"              TEXT,
      "filetype"                TEXT,
      "file"                    TEXT,
      "checksum"                TEXT,
      "quarskip"                TEXT,
      "virus"                   TEXT,
      "ref"                     TEXT,
      "url"                     TEXT,
      "endpoint"                TEXT,
      "profile"                 TEXT,
      "user"                    TEXT,
      "group"                   TEXT,
      "agent"                   TEXT,
      "from"                    TEXT,
      "to"                      TEXT,
      "command"                 TEXT,
      "dtype"                   TEXT
)
```

Web Filter log

```
CREATE TABLE webfilter_log
(
      "oid"                     INTEGER PRIMARY KEY AUTOINCREMENT,
      "timestamp"               INTEGER,
      "log_id"                  INTEGER,
      "subtype"                 TEXT,
      "pri"                     TEXT,
      "policyid"                INTEGER,
      "serial"                  INTEGER,
      "user"                    TEXT,
      "group"                   TEXT,
      "src"                     TEXT,
      "sport"                   INTEGER,
```

```
        "src_int"               TEXT,
        "dst"                   TEXT,
        "dport"                 INTEGER,
        "dst_int"               TEXT,
        "service"               TEXT,
        "hostname"              TEXT,
        "carrier_ep"            TEXT,
        "profile"               TEXT,
        "status"                TEXT,
        "req_type"              TEXT,
        "url"                   TEXT,
        "msg"                   TEXT,
        "dir"                   TEXT,
        "agent"                 TEXT,
        "from"                  TEXT,
        "to"                    TEXT,
        "banword"               TEXT,
        "error"                 TEXT,
        "method"                TEXT,
        "class"                 INTEGER,
        "class_desc"            TEXT,
        "cat"                   INTEGER,
        "cat_desc"              TEXT,
        "mode"                  TEXT,
        "rule_type"             TEXT,
        "rule_data"             TEXT,
        "ovrd_tbl"              TEXT,
        "ovrd_id"               INTEGER,
        "count"                 INTEGER,
        "url_type"              TEXT
)
```

Spam filter or email filter log

```
CREATE TABLE spamfilter_log
(
        "oid"                   INTEGER PRIMARY KEY AUTOINCREMENT,
        "timestamp"             INTEGER,
        "log_id"                INTEGER,
        "subtype"               TEXT,
        "pri"                   TEXT,
        "policyid"              INTEGER,
        "serial"                INTEGER,
        "user"                  TEXT,
        "group"                 TEXT,
        "src"                   TEXT,
        "sport"                 INTEGER,
        "src_int"               TEXT,
        "dst"                   TEXT,
        "dport"                 INTEGER,
        "dst_int"               TEXT,
        "service"               TEXT,
        "carrier_ep"            TEXT,
        "profile"               TEXT,
```

```
        "status"                TEXT,
        "from"                  TEXT,
        "to"                    TEXT,
        "banword"               TEXT,
        "tracker"               TEXT,
        "dir"                   TEXT,
        "agent"                 TEXT,
        "msg"                   TEXT
)
```

DLP log

```
CREATE TABLE dlp_log
(
        "oid"                   INTEGER PRIMARY KEY AUTOINCREMENT,
        "timestamp"             INTEGER,
        "log_id"                INTEGER,
        "subtype"               TEXT,
        "pri"                   TEXT,
        "policyid"              INTEGER,
        "serial"                INTEGER,
        "user"                  TEXT,
        "group"                 TEXT,
        "src"                   TEXT,
        "sport"                 INTEGER,
        "src_int"               TEXT,
        "dst"                   TEXT,
        "dport"                 INTEGER,
        "dst_int"               TEXT,
        "service"               TEXT,
        "status"                TEXT,
        "hostname"              TEXT,
        "url"                   TEXT,
        "from"                  TEXT,
        "to"                    TEXT,
        "msg"                   TEXT,
        "rulename"              TEXT,
        "compoundname"          TEXT,
        "action"                TEXT,
        "severity"              INTEGER
)
```

Application control log

```
CREATE TABLE app_control_log
(
        "oid"                   INTEGER PRIMARY KEY AUTOINCREMENT,
        "timestamp"             INTEGER,
        "log_id"                INTEGER,
        "subtype"               TEXT,
        "pri"                   TEXT,
        "user"                  TEXT,
        "group"                 TEXT,
        "carrier_ep"            TEXT,
        "kind"                  TEXT,
```

```
        "profile"               TEXT,
        "dir"                   TEXT,
        "src"                   TEXT,
        "src_port"              INTEGER,
        "src_int"               TEXT,
        "dst"                   TEXT,
        "dst_port"              INTEGER,
        "dst_int"               TEXT,
        "src_name"              TEXT,
        "dst_name"              TEXT,
        "proto"                 INTEGER,
        "service"               TEXT,
        "policyid"              INTEGER,
        "serial"                INTEGER,
        "app_list"              TEXT,
        "app_type"              TEXT,
        "app"                   TEXT,
        "action"                TEXT,
        "status"                TEXT,
        "count"                 INTEGER,
        "filename"              TEXT,
        "filesize"              INTEGER,
        "message"               TEXT,
        "content"               TEXT,
        "reason"                TEXT,
        "req"                   TEXT,
        "phone"                 TEXT,
        "msg"                   TEXT
)
```

router

Routers move packets from one network segment to another towards a network destination. When a packet reaches a router, the router uses data in the packet header to look up a suitable route on which to forward the packet to the next segment. The information that a router uses to make routing decisions is stored in a routing table. Other factors related to the availability of routes and the status of the network may influence the route selection that a router makes when forwarding a packet to the next segment.

The FortiGate unit supports many advanced routing functions and is compatible with industry standard Internet routers. The FortiGate unit can communicate with other routers to determine the best route for a packet.

The following `router` commands are available to configure options related to FortiGate unit router communications and packet forwarding:

access-list, access-list6	key-chain	rip
aspath-list	multicast	ripng
auth-path	ospf	route-map
bgp	ospf6	setting
community-list	policy	static
	prefix-list, prefix-list6	static6

access-list, access-list6

Use this command to add, edit, or delete access lists. Access lists are filters used by FortiGate unit routing processes. For an access list to take effect, it must be called by a FortiGate unit routing process (for example, a process that supports RIP or OSPF). Use `access-list6` for IPv6 routing.

Each rule in an access list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and whether to match the prefix exactly or to match the prefix and any more specific prefix.

Note: If you are setting a prefix of 128.0.0.0, use the format 128.0.0.0/1. The default route, 0.0.0.0/0 can not be exactly matched with an access-list. A prefix-list must be used for this purpose. For more information, see "prefix-list, prefix-list6" on page 337.

The FortiGate unit attempts to match a packet against the rules in an access list starting at the top of the list. If it finds a match for the prefix, it takes the action specified for that prefix. If no match is found the default action is deny.

Syntax

```
config router access-list, access-list6
  edit <access_list_name>
    set comments <string>
    config rule
      edit <access_list_id>
        set action {deny | permit}
        set exact-match {enable | disable}
        set prefix { <prefix_ipv4mask> | any }
        set prefix6 { <prefix_ipv6mask> | any }
        set wildcard <address_ipv4> <wildcard_mask>
      end
    end
```

Note: The `action` and `prefix` fields are required. The `exact-match` field is optional.

Variable	Description	Default
`edit <access_list_name>`	Enter a name for the access list. An access list and a prefix list cannot have the same name.	No default.
`comments <string>`	Enter a descriptive comment. The max length is 127 characters.	No default.
config rule variables		
`edit <access_list_id>`	Enter an entry number for the rule. The number must be an integer.	No default.
`action {deny | permit}`	Set the action to take for this prefix.	`permit`
`exact-match {enable | disable}`	By default, access list rules are matched on the prefix or any more specific prefix. Enable `exact-match` to match only the configured prefix.	`disable`
`prefix { <prefix_ipv4mask> | any }`	Enter the prefix for this access list rule. Enter either: **`IPv4 address and network mask`** **`any`** — match any prefix.	`any`

Variable	Description	Default
`prefix6 { <prefix_ipv6mask> | any }`	Enter the prefix for this IPv6 access list rule. Enter either: **`IPv6 address and network mask`** **`any`** — match any prefix. This variable is only used with `config access-list6`.	`any`
`wildcard <address_ipv4> <wildcard_mask>`	Enter the IP address and reverse (wildcard) mask to process. The value of the mask (for example, `0.0.255.0`) determines which address bits to match. A value of 0 means that an exact match is required, while a binary value of 1 indicates that part of the binary network address does not have to match. You can specify discontinuous masks (for example, to process "even" or "odd" networks according to any network address octet). For best results, do not specify a `wildcard` attribute unless `prefix` is set to `any`. This variable is only used with `config access-list`.	No default.

Example

This example shows how to add an access list named `acc_list1` with two rules. The first rule denies the subnet that exactly matches the prefix `192.168.50.0 255.255.255.0` and permits all other subnets that match the prefix `192.168.0.0 255.255.0.0`.

```
config router access-list
  edit acc_list1
    config rule
      edit 1
        set prefix 192.168.50.0 255.255.255.0
        set action deny
        set exact-match enable
      next
      edit 2
        set prefix 192.168.0.0 255.255.0.0
        set action permit
        set exact-match disable
      end
    end
```

When using IPv6 addresses, there is no space between the address and the netmask. The same example using IPv6 addresses would be:

```
config router access-list6
  edit acc_list_ip6_1
    config rule
      edit 1
        set prefix6 2002:C0A8:3200:0:0:0:0:0/28
        set action deny
        set exact-match enable
      next
      edit 2
        set prefix6 2002:C0A8:0:0:0:0:0:0/28
        set action permit
        set exact-match disable
      end
    end
```

The next example shows how to add an access list that permits all subnets matching network address 10.20.4.1 through 10.20.4.255 (addresses 10.20.4.x are processed):

```
config router access-list
  edit acc_list2
    config rule
      edit 1
        set action permit
        set wildcard 10.20.4.0 0.0.0.255
      end
    end
```

The next example shows how to add an access list that permits “odd” subnets according to the third-octet of network address 172.16.x.0 (networks 172.16.1.0, 172.16.3.0, 172.16.5.0, and so on are processed):

```
config router access-list
  edit acc_list3
    config rule
      edit 1
        set action permit
        set wildcard 172.16.1.0 0.0.254.0
      end
    end
```

History

FortiOS v2.80 New.

FortiOS v3.0 Added `wildcard` attribute. Changed `exact_match` field to `exact-match`.

FortiOS v3.0 MR6 Added `comments` attribute.

FortiOS v4.0 MR1 Added `access-list6` command, `prefix6` attribute.

Related topics

- router ospf
- router prefix-list, prefix-list6
- router rip

aspath-list

Use this command to set or unset BGP AS-path list parameters. By default, BGP uses an ordered list of Autonomous System (AS) numbers to describe the route that a packet takes to reach its destination. A list of these AS numbers is called the AS path. You can filter BGP routes using AS path lists.

When the FortiGate unit receives routing updates from other autonomous systems, it can perform operations on updates from neighbors and choose the shortest path to a destination. The shortest path is determined by counting the AS numbers in the AS path. The path that has the least AS numbers is considered the shortest AS path.

Use the `config router aspath-list` command to define an access list that examines the AS_PATH attributes of BGP routes to match routes. Each entry in the AS-path list defines a rule for matching and selecting routes based on the setting of the AS_PATH attribute. The default rule in an AS path list (which the FortiGate unit applies last) denies the matching of all routes.

Syntax

```
config router aspath-list
  edit <aspath_list_name>
    config rule
    edit <as_rule_id>
      set action {deny | permit}
      set regexp <regexp_str>
    end
  end
```

Note: The `action` and `regexp` fields are required.

Variable	Description	Default
`edit <aspath_list_name>`	Enter a name for the AS path list.	No default.
config rule variables		
`edit <as_rule_id>`	Enter an entry number for the rule. The number must be an integer.	No default.
`action {deny | permit}`	Deny or permit operations on a route based on the value of the route's AS_PATH attribute.	No default.
`regexp <regexp_str>`	Specify the regular expression that will be compared to the AS_PATH attribute (for example, `^730$`). The value is used to match AS numbers. Delimit a complex `regexp_str` value using double-quotation marks.	`Null.`

Example

This example shows how to create an AS-path list named `ebgp_in that allows AS_PATHs from a group of 4 systems`. The list contains a single rule that permits operations on BGP routes whose AS_PATH attribute references an AS number of 333, 334, 338, or 71. The AS path list will match routes that originate in AS 333, AS 334, AS 338, or AS 71.

```
config router aspath-list
  edit ebgp_in
    config rule
      edit 1
        set action permit
        set regexp _(333|334|338|71)$
      end
  end
```

History

FortiOS v3.0 New.

Related topics

- router bgp
- router community-list
- Using route maps with BGP
- router key-chain

auth-path

Authentication based routing allows firewall policies to direct network traffic flows.

This command configures a RADIUS object on your FortiGate unit. The same object is required to be configured on the RADIUS server.

To configure authentication based routing on your FortiGate unit

1. Configure your FortiGate unit to communicate with a RADIUS authentication server.
2. Configure a user that uses the RADIUS server.
3. Add that user to a user group configured to use the RADIUS server.
4. Configure the router `auth-path` object.
5. Configure a custom service for RADIUS traffic.
6. Configure a service group that includes RADIUS traffic along with other types of traffic that will be allowed to pass through the firewall.
7. Configure a firewall policy that has route based authentication enabled.

The Fortinet Knowledge Base has an article on authentication based routing that provides a sample configuration for these steps.

Note: The `auth-path` command is not available when the FortiGate unit is in Transparent mode.

Syntax

```
config router auth-path
  edit <aspath_list_name>
    set device <interface>
    set gateway <gway_ipv4>
  end
```

Variable	Description	Default
`edit <auth_path_name>`	Enter a name for the authentication path.	No default.
`device <interface>`	Specify the interface for this path.	No default.
`gateway <gway_ipv4>`	Specify the gateway IP address for this path.	`Null`.

Example

This example shows how to configure an auth-path object called `auth_route` that routes traffic over the dmz interface using 172.20.120.4. These settings also need to be configured on the RADIUS server used to authenticate.

```
config router auth-path
  edit auth_route
    set device dmz
    set gateway 172.20.120.4
  next
end
```

History

FortiOS v3.0 MR6 New.

Related topics

- user local
- user radius
- firewall policy, policy6

bgp

Use this command to set or unset BGP-4 routing parameters. BGP can be used to perform Classless Interdomain Routing (CIDR) and to route traffic between different autonomous systems or domains using an alternative route if a link between a FortiGate unit and a BGP peer (such as an ISP router) fails. FortiOS BGP4 complies with RFC 1771 and supports IPv4 addressing.

FortiOS supports IPv6 over BGP4 via the BGP4+ protocol defined in RFC 2545, and RFC 2858. IPv6 configuration for BGP is accomplished with the `aggregate-address6`, `network6`, and `redistribute6` variables. Also almost every variable in `config neighbour` has an IPv4 and IPv6 version such as `activate` and `activate6`. Any variable ending with a “6” is an IPv6 variable.

When BGP is enabled, the FortiGate unit sends routing table updates to the upstream ISP router whenever any part of the routing table changes. The update advertises which routes can be used to reach the FortiGate unit. In this way, routes are made known from the border of the internal network outwards (routes are pushed forward) instead of relying on upstream routers to propagate alternative paths to the FortiGate unit.

FortiGate unit BGP supports the following extensions to help manage large numbers of BGP peers:

- Communities — The FortiGate unit can set the COMMUNITY attribute of a route to assign the route to predefined paths (see RFC 1997). The FortiGate unit can examine the COMMUNITY attribute of learned routes to perform local filtering and/or redistribution.
- Internal BGP (IBGP) route reflectors — The FortiGate unit can operate as a route reflector or participate as a client in a cluster of IBGP peers (see RFC 1966).
- External BGP (EBGP) confederations — The FortiGate unit can operate as a confederation member, using its AS confederation identifier in all transactions with peers that are not members of its confederation (see RFC 3065).

Bi-directional Forwarding Detection (BFD) is a protocol used by BGP, and OSPF. It is used to quickly locate hardware failures in the network. Routers running BFD send unicast messages to each other, and if a timer runs out, meaning no messages have been received, on a connection then that unresponsive router is declared down. BFD then communicates this information to the routing protocol and the routing information is updated. BFD support can only be configured through the CLI.

Syntax

```
config router bgp
  set always-compare-med {enable | disable}
  set as <local_as_id>
  set bestpath-as-path-ignore {enable | disable}
  set bestpath-cmp-confed-aspath {enable | disable}
  set bestpath-cmp-routerid {enable | disable}
  set bestpath-med-confed {enable | disable}
  set bestpath-med-missing-as-worst {enable | disable}
  set client-to-client-reflection {enable | disable}
  set cluster-id <address_ipv4>
  set confederation-identifier <peerid_integer>
  set dampening {enable | disable}
  set dampening-max-suppress-time <minutes_integer>
  set dampening-reachability-half-life <minutes_integer>
  set dampening-reuse <reuse_integer>
  set dampening-route-map <routemap-name_str>
  set dampening-suppress <limit_integer>
  set dampening-unreachability-half-life <minutes_integer>
  set default-local-preference <preference_integer>
  set deterministic-med {enable | disable}
```

```
set distance-external <distance_integer>
set distance-internal <distance_integer>
set distance-local <distance_integer>
set enforce-first-as {enable | disable}
set fast-external-failover {enable | disable}
set graceful_restart {enable | disable}
set holdtime-timer <seconds_integer>
set ignore_optional_capability {enable | disable}
set keepalive-timer <seconds_integer>
set log-neighbor-changes {enable | disable}
set network-import-check {enable | disable}
set router-id <address_ipv4>
set scan-time <seconds_integer>
set synchronization {enable | disable}
config admin-distance
  edit <route_entry_id>
    set distance <integer>
    set neighbor-prefix <ip_and_netmask>
    set route-list <string>
  end
config aggregate-address
  edit <aggr_addr_id>
    set as-set {enable | disable}
    set prefix <address_ipv4mask>
    set summary-only {enable | disable}
  end
config aggregate-address6
  edit <aggr_addr_id>
    set as-set {enable | disable}
    set prefix6 <address_ipv6mask>
    set summary-only {enable | disable}
  end
config neighbor
  edit <neighbor_address_ipv4>
    set activate {enable | disable}
    set activate6 {enable | disable}
    set advertisement-interval <seconds_integer>
    set allowas-in <max_num_AS_integer>
    set allowas-in6 <max_num_AS_integer>
    set allowas-in-enable {enable | disable}
    set allowas-in-enable6 {enable | disable}
    set attribute-unchanged [as-path] [med] [next-hop]
    set attribute-unchanged6 [as-path] [med] [next-hop]
    set bfd {enable | disable}
    set capability-default-originate {enable | disable}
    set capability-default-originate6 {enable | disable}
    set capability-dynamic {enable | disable}
    set capability-graceful-restart {enable | disable}
    set capability-graceful-restart6 {enable | disable}
    set capability-orf {both | none | receive | send}
    set capability-orf6 {both | none | receive | send}
    set capability-route-refresh {enable | disable}
    set connect-timer <seconds_integer>
    set default-originate-routemap <routemap_str>
```

```
      set default-originate-routemap6 <routemap_str>
      set description <text_str>
      set distribute-list-in <access-list-name_str>
      set distribute-list-in6 <access-list-name_str>
      set distribute-list-out <access-list-name_str>
      set distribute-list-out6 <access-list-name_str>
      set dont-capability-negotiate {enable | disable}
      set ebgp-enforce-multihop {enable | disable}
      set ebgp-multihop-ttl <seconds_integer>
      set filter-list-in <aspath-list-name_str>
      set filter-list-in6 <aspath-list-name_str>
      set filter-list-out <aspath-list-name_str>
      set filter-list-out6 <aspath-list-name_str>
      set holdtime-timer <seconds_integer>
      set interface <interface-name_str>
      set keep-alive-timer <seconds_integer>
      set maximum-prefix <prefix_integer>
      set maximum-prefix6 <prefix_integer>
      set maximum-prefix-threshold <percentage_integer>
      set maximum-prefix-threshold6 <percentage_integer>
      set maximum-prefix-warning-only {enable | disable}
      set maximum-prefix-warning-only6 {enable | disable}
      set next-hop-self {enable | disable}
      set next-hop-self6 {enable | disable}
      set override-capability {enable | disable}
      set passive {enable | disable}
      set password <string>
      set prefix-list-in <prefix-list-name_str>
      set prefix-list-in6 <prefix-list-name_str>
      set prefix-list-out <prefix-list-name_str>
      set prefix-list-out6 <prefix-list-name_str>
      set remote-as <id_integer>
      set remove-private-as {enable | disable}
      set remove-private-as6 {enable | disable}
      set retain-stale-time <seconds_integer>
      set route-map-in <routemap-name_str>
      set route-map-in6 <routemap-name_str>
      set route-map-out <routemap-name_str>
      set route-map-out6 <routemap-name_str>
      set route-reflector-client {enable | disable}
      set route-reflector-client6 {enable | disable}
      set route-server-client {enable | disable}
      set route-server-client6 {enable | disable}
      set send-community {both | disable | extended | standard}
      set send-community6 {both | disable | extended | standard}
      set shutdown {enable | disable}
      set soft-reconfiguration {enable | disable}
      set strict-capability-match {enable | disable}
      set unsuppress-map <route-map-name_str>
      set update-source <interface-name_str>
      set weight <weight_integer>
    end
  config network
    edit <network_id>
```

```
      set backdoor {enable | disable}
      set prefix <address_ipv4mask>
      set route-map <routemap-name_str>
    end
  config network6
    edit <network_id>
      set backdoor {enable | disable}
      set prefix6 <address_ipv6mask>
      set route-map <routemap-name_str>
    end
  config redistribute {connected | static | rip | ospf}
    set status {enable | disable}
    set route-map <route-map-name_str>
  end
  config redistribute6 {connected | static | rip | ospf}
    set status {enable | disable}
    set route-map <route-map-name_str>
  end
end
```

config router bgp

Use this command to enable a Border Gateway Protocol version 4 (BGP-4) process on the FortiGate unit, define the interfaces making up the local BGP network (see "config network" on page 296), and set operating parameters for communicating with BGP neighbors (see "config neighbor" on page 290).

When multiple routes to the FortiGate unit exist, BGP attributes determine the best route and the FortiGate unit communicates this information to its BGP peers. The best route is added to the IP routing table of the BGP peer, which in turn propagates this updated routing information to upstream routers.

FortiGate units maintain separate entries in their routing tables for BGP routes. See "Using route maps with BGP" on page 356. To reduce the size of the BGP routing table and conserve network resources, you can optionally aggregate routes to the FortiGate unit. An aggregate route enables the FortiGate unit to advertise one block of contiguous IP addresses as a single, less-specific address. You can implement aggregate routing either by redistributing an aggregate route (see "config redistribute" on page 297) or by using the conditional aggregate routing feature (see "config aggregate-address" on page 289).

Note: In the following table, the `as` and `router-id` fields are required. All other fields are optional.

Variable	Description	Default
`always-compare-med {enable | disable}`	Enable or disable the comparison of MULTI_EXIT_DISC (Multi Exit Discriminator or MED) attributes for identical destinations advertised by BGP peers in different autonomous systems.	`disable`
`as <local_as_id>`	Enter an integer to specify the local autonomous system (AS) number of the FortiGate unit. The range is from 1 to 65 535. When the `local_as_id` number is different than the AS number of the specified BGP neighbor (see "remote-as <id_integer>" on page 294), an External BGP (EBGP) session is started. Otherwise, an Internal BGP (IBGP) session is started. A value of `0` is not allowed.	`0`
`bestpath-as-path-ignore {enable | disable}`	Enable or disable the inclusion of an AS path in the selection algorithm for choosing a BGP route.	`disable`
`bestpath-cmp-confed-aspath {enable | disable}`	Enable or disable the comparison of the AS_CONFED_SEQUENCE attribute, which defines an ordered list of AS numbers representing a path from the FortiGate unit through autonomous systems within the local confederation.	`disable`

Variable	Description	Default
bestpath-cmp-routerid {enable | disable}	Enable or disable the comparison of the router-ID values for identical EBGP paths.	disable
bestpath-med-confed {enable | disable}	Enable or disable the comparison of MED attributes for routes advertised by confederation EBGP peers.	disable
bestpath-med-missing-as-worst {enable | disable}	This field is available when bestpath-med-confed is set to enable. When bestpath-med-confed is enabled, treat any confederation path with a missing MED metric as the least preferred path.	disable
client-to-client-reflection {enable | disable}	Enable or disable client-to-client route reflection between IBGP peers. If the clients are fully meshed, route reflection may be disabled.	enable
cluster-id <address_ipv4>	Set the identifier of the route-reflector in the cluster ID to which the FortiGate unit belongs. If 0 is specified, the FortiGate unit operates as the route reflector and its router-id value is used as the cluster-id value. If the FortiGate unit identifies its own cluster ID in the CLUSTER_LIST attribute of a received route, the route is ignored to prevent looping.	0.0.0.0
confederation-identifier <peerid_integer>	Set the identifier of the confederation to which the FortiGate unit belongs. The range is from 1 to 65 535.	0
dampening {enable | disable}	Enable or disable route-flap dampening on all BGP routes. See RFC 2439. (A flapping route is unstable and continually transitions down and up.) If you set dampening, you may optionally set dampening-route-map or define the associated values individually using the dampening-* fields.	disable
dampening-max-suppress-time <minutes_integer>	This field is available when dampening is set to enable. Set the maximum time (in minutes) that a route can be suppressed. The range is from 1 to 255. A route may continue to accumulate penalties while it is suppressed. However, the route cannot be suppressed longer than minutes_integer.	60
dampening-reachability-half-life <minutes_integer>	This field is available when dampening is set to enable. Set the time (in minutes) after which any penalty assigned to a reachable (but flapping) route is decreased by half. The range is from 1 to 45.	15
dampening-reuse <reuse_integer>	This field is available when dampening is set to enable. Set a dampening-reuse limit based on accumulated penalties. The range is from 1 to 20 000. If the penalty assigned to a flapping route decreases enough to fall below the specified reuse_integer, the route is not suppressed.	750
dampening-route-map <routemap-name_str>	This field is available when dampening is set to enable. Specify the route-map that contains criteria for dampening. You must create the route-map before it can be selected here. See “route-map” on page 354 and “Using route maps with BGP” on page 356.	Null.
dampening-suppress <limit_integer>	This field is available when dampening is set to enable. Set a dampening-suppression limit. The range is from 1 to 20 000. A route is suppressed (not advertised) when its penalty exceeds the specified limit.	2 000
dampening-unreachability-half-life <minutes_integer>	This field is available when dampening is set to enable. Set the time (in minutes) after which the penalty on a route that is considered unreachable is decreased by half. The range is from 1 to 45.	15
default-local-preference <preference_integer>	Set the default local preference value. A higher value signifies a preferred route. The range is from 0 to 4 294 967 295.	100
deterministic-med {enable | disable}	Enable or disable deterministic comparison of the MED attributes of routes advertised by peers in the same AS.	disable

Variable	Description	Default
distance-external <distance_integer>	Set the administrative distance of EBGP routes. The range is from 1 to 255. If you set this value, you must also set values for distance-internal and distance-local.	20
distance-internal <distance_integer>	This field is available when distance-external is set. Set the administrative distance of IBGP routes. The range is from 1 to 255.	200
distance-local <distance_integer>	This field is available when distance-external is set. Set the administrative distance of local BGP routes. The range is from 1 to 255.	200
enforce-first-as {enable | disable}	Enable or disable the addition of routes learned from an EBGP peer when the AS number at the beginning of the route's AS_PATH attribute does not match the AS number of the EBGP peer.	disable
fast-external-failover {enable | disable}	Immediately reset the session information associated with BGP external peers if the link used to reach them goes down.	enable
graceful_restart {enable | disable}	Graceful restart capability limits the effects of software problems by allowing forwarding to continue when the control plane of the router fails. It also reduces routing flaps by stabilizing the network.	disable
holdtime-timer <seconds_integer>	The maximum amount of time (in seconds) that may expire before the FortiGate unit declares any BGP peer down. A keepalive message must be received every seconds_integer seconds, or the peer is declared down. The value can be 0 or an integer in the 3 to 65 535 range.	180
ignore_optional_capability {enable | disable}	Don't send unknown optional capability notification message.	disable
keepalive-timer <seconds_integer>	The frequency (in seconds) that a keepalive message is sent from the FortiGate unit to any BGP peer. The range is from 0 to 65 535. BGP peers exchange keepalive messages to maintain the connection for the duration of the session.	60
log-neighbor-changes {enable | disable}	Enable or disable the logging of changes to BGP neighbor status.	disable
network-import-check {enable | disable}	Enable or disable the advertising of the BGP network in IGP (see "config network" on page 296).	enable
router-id <address_ipv4>	Specify a fixed identifier for the FortiGate unit. A value of 0.0.0.0 is not allowed. If router-id is not explicitly set, the highest IP address of the VDOM will be used as the default router-id.	0.0.0.0
scan-time <seconds_integer>	Configure the background scanner interval (in seconds) for next-hop route scanning. The range is from 5 to 60.	60
synchronization {enable | disable}	Only advertise routes from iBGP if routes are present in an interior gateway protocol (IGP) such as RIP or OSPF.	disable

Example

The following example defines the number of the AS of which the FortiGate unit is a member. It also defines an EBGP neighbor at IP address 10.0.1.2.

```
config router bgp
  set as 65001
  set router-id 172.16.120.20
  config neighbor
    edit 10.0.1.2
      set remote-as 65100
    end
  end
```

config admin-distance

Use this subcommand to set administrative distance modifications for bgp routes.

Variable	Description	Default
`edit <route_entry_id>`	Enter an ID number for the entry. The number must be an integer.	No default.
`distance <integer>`	The administrative distance to apply to the route. This value can be from 1 to 255.	No default.
`neighbor-prefix <ip_and_netmask>`	Neighbor address prefix. This variable must be a valid IP address and netmask.	No default.
`route-list <string>`	The list of routes this distance will be applied to. The routes in this list can only come from the access-list which can be viewed at `config router access-list`.	No default.

Example

This example shows how to manually adjust the distance associated with a route. It shows adding 25 to the weight of the route, that it will apply to neighbor routes with an IP address of 192.168.0.0 and a netmask of 255.255.0.0, that are also permitted by the access-list “downtown_office”.

```
config router bgp
  config admin-distance
    edit 1
      set distance 25
      set neighbour-prefix 192.168.0.0 255.255.0.0
      set route-list downtown_office
    next
  end
end
```

config aggregate-address

config aggregate-address6

Use this subcommand to set or unset BGP aggregate-address table parameters. The subcommand creates a BGP aggregate entry in the FortiGate unit routing table. Use `config aggregate-address6` for IPv6 routing.

When you aggregate routes, routing becomes less precise because path details are not readily available for routing purposes. The aggregate address represents addresses in several autonomous systems. Aggregation reduces the length of the network mask until it masks only the bits that are common to all of the addresses being summarized.

Note: The `prefix` field is required. All other fields are optional.

Variable	Description	Default
`edit <aggr_addr_id>`	Enter an ID number for the entry. The number must be an integer.	No default.
`as-set {enable | disable}`	Enable or disable the generation of an unordered list of AS numbers to include in the path information. When `as-set` is enabled, a `set-atomic-aggregate` value (see “Using route maps with BGP” on page 356) does not have to be specified.	`disable`
`prefix <address_ipv4mask>`	Set an aggregate prefix. Include the IP address and netmask.	`0.0.0.0 0.0.0.0`

Variable	Description	Default
prefix6 <address_ipv6mask>	Set an aggregate IPv6 prefix. Include the IP address and netmask.	::/0
summary-only {enable | disable}	Enable or disable the advertising of aggregate routes only (the advertising of specific routes is suppressed).	disable

Example

This example shows how to define an aggregate prefix of 192.168.0.0/16. The as-set command enables the generation of an unordered list of AS numbers to include in the path information.

```
config router bgp
  config aggregate-address
    edit 1
      set prefix 192.168.0.0/16
      set as-set enable
    end
  end
```

config neighbor

Use this subcommand to set or unset BGP neighbor configuration settings. The subcommand adds a BGP neighbor configuration to the FortiGate unit.

You can add up to 1000 BGP neighbors, and optionally use MD5 authentication to password protect BGP sessions with those neighbors. (see RFC 2385)

You can clear all or some BGP neighbor connections (sessions) using the exec router clear bgp command (see “router clear bgp” on page 732).

Note: The remote-as field is required. All other fields are optional.

Variable	Description	Default
edit <neighbor_address_ipv4>	Enter the IP address of the BGP neighbor. You can have up to 1000 configured neighbors.	No default.
activate {enable | disable}	Enable or disable the address family for the BGP neighbor.	enable
activate6 {enable | disable}	Enable or disable the address family for the BGP neighbor (IPv6).	enable
advertisement-interval <seconds_integer>	Set the minimum amount of time (in seconds) that the FortiGate unit waits before sending a BGP routing update to the BGP neighbor. The range is from 0 to 600.	30
allowas-in <max_num_AS_integer>	This field is available when allowas-in-enable is set to enable. Set the maximum number of occurrences your AS number is allowed in. When allowas-in-enable is disabled, your AS number is only allowed to appear once in an AS_PATH. .	unset
allowas-in6 <max_num_AS_integer>	This field is available when allowas-in-enable6 is set to enable. When allowas-in-enable6 is disabled, your AS number is only allowed to appear once in an AS_PATH. Set the maximum number of occurrences your AS number is allowed in.	unset

Variable	Description	Default
`allowas-in-enable {enable | disable}`	Enable or disable the readvertising of all prefixes containing duplicate AS numbers. Set the amount of time that must expire before readvertising through the `allowas-in` field.	`disable`
`allowas-in-enable6 {enable | disable}`	Enable or disable the readvertising of all prefixes containing duplicate AS numbers. Set the amount of time that must expire before readvertising through the `allowas-in6` field.	`disable`
`attribute-unchanged [as-path] [med] [next-hop]`	Propagate unchanged BGP attributes to the BGP neighbor. • To advertise unchanged AS_PATH attributes, select `as-path`. • To advertise unchanged MULTI_EXIT_DISC attributes, select `med`. • To advertise the IP address of the next-hop router interface (even when the address has not changed), select `next-hop`. • An empty set is a supported value.	Empty set.
`attribute-unchanged6 [as-path] [med] [next-hop]`	Propagate unchanged BGP attributes to the BGP neighbor. • To advertise unchanged AS_PATH attributes, select `as-path`. • To advertise unchanged MULTI_EXIT_DISC attributes, select `med`. • To advertise the IP address of the next-hop router interface (even when the address has not changed), select `next-hop`. • An empty set is a supported value.	Empty set.
`bfd {enable | disable}`	Enable to turn on Bi-Directional Forwarding Detection (BFD) for this neighbor. This indicates that this neighbor is using BFD.	`disable`
`capability-default-originate {enable | disable}`	Enable or disable the advertising of the default route to BGP neighbors.	`disable`
`capability-default-originate6 {enable | disable}`	Enable or disable the advertising of the default route to IPv6 BGP neighbors.	`disable`
`capability-dynamic {enable | disable}`	Enable or disable the advertising of dynamic capability to BGP neighbors.	`disable`
`capability-graceful-restart {enable | disable}`	Enable or disable the advertising of graceful-restart capability to BGP neighbors.	`disable`
`capability-graceful-restart6 {enable | disable}`	Enable or disable the advertising of graceful-restart capability to IPv6 BGP neighbors.	`disable`
`capability-orf {both | none | receive | send}`	Enable advertising of Outbound Routing Filter (ORF) prefix-list capability to the BGP neighbor. Choose one of: **`both`** — enable send and receive capability. **`receive`** — enable receive capability. **`send`** — enable send capability. **`none`** — disable the advertising of ORF prefix-list capability. •	`disable`
`capability-orf6 {both | none | receive | send}`	Enable advertising of IPv6 ORF prefix-list capability to the BGP neighbor. Choose one of: **`both`** — enable send and receive capability. **`receive`** — enable receive capability. **`send`** — enable send capability. **`none`** — disable the advertising of IPv6 ORF prefix-list capability.	`disable`
`capability-route-refresh {enable | disable}`	Enable or disable the advertising of route-refresh capability to the BGP neighbor.	`enable`

Variable	Description	Default
connect-timer <seconds_integer>	Set the maximum amount of time (in seconds) that the FortiGate unit waits to make a connection with a BGP neighbor before the neighbor is declared unreachable. The range is from 0 to 65 535.	-1 (not set)
default-originate-routemap <routemap_str>	Advertise a default route out from the FortiGate unit to this neighbor using a route_map named <routemap_str>. The route_map name can be up to 35 characters long and is defined using the config router route_map command. For more information, see "router route-map" on page 354.	Null.
default-originate-routemap6 <routemap_str>	Advertise a default route out from the FortiGate unit to this neighbor using a route_map named <routemap_str>. The route_map name can be up to 35 characters long and is defined using the config router route_map command.	Null.
description <text_str>	Enter a one-word (no spaces) description to associate with the BGP neighbor configuration settings.	Null.
distribute-list-in <access-list-name_str>	Limit route updates from the BGP neighbor based on the Network Layer Reachability Information (NLRI) defined in the specified access list. You must create the access list before it can be selected here. See "access-list, access-list6" on page 276.	Null.
distribute-list-in6 <access-list-name_str>	Limit route updates from the IPv6 BGP neighbor based on the Network Layer Reachability Information (NLRI) defined in the specified access list. You must create the access list before it can be selected here. See "access-list, access-list6" on page 276.	Null
distribute-list-out <access-list-name_str>	Limit route updates to the BGP neighbor based on the NLRI defined in the specified access list. You must create the access list before it can be selected here. See "access-list, access-list6" on page 276.	Null.
distribute-list-out6 <access-list-name_str>	Limit route updates to the IPv6 BGP neighbor based on the NLRI defined in the specified access list. You must create the access list before it can be selected here. See "access-list, access-list6" on page 276.	Null
dont-capability-negotiate {enable | disable}	Enable or disable capability negotiations with the BGP neighbor.	disable
ebgp-enforce-multihop {enable | disable}	Enable or disable the enforcement of Exterior BGP (EBGP) multihops.	disable
ebgp-multihop-ttl <seconds_integer>	This field is available when ebgp-multihop is set to enable. Define a TTL value (in hop counts) for BGP packets sent to the BGP neighbor. The range is from 1 to 255.	255
filter-list-in <aspath-list-name_str>	Limit inbound BGP routes according to the specified AS-path list. You must create the AS-path list before it can be selected here. See "aspath-list" on page 279.	Null.
filter-list-in6 <aspath-list-name_str>	Limit inbound IPv6 BGP routes according to the specified AS-path list. You must create the AS-path list before it can be selected here. See config router aspath-list.	Null
filter-list-out <aspath-list-name_str>	Limit outbound BGP routes according to the specified AS-path list. You must create the AS-path list before it can be selected here. See "router aspath-list" on page 279.	Null.
filter-list-out6 <aspath-list-name_str>	Limit outbound IPv6 BGP routes according to the specified AS-path list. You must create the AS-path list before it can be selected here. See config router aspath-list.	Null

Variable	Description	Default
holdtime-timer <seconds_integer>	The amount of time (in seconds) that must expire before the FortiGate unit declares the BGP neighbor down. This value overrides the global holdtime-timer value (see "holdtime-timer <seconds_integer>" on page 288). A keepalive message must be received every seconds_integer from the BGP neighbor or it is declared down. The value can be 0 or an integer in the 3 to 65 535 range. This field is available when graceful-restart is set to enabled.	-1 (not set)
interface <interface-name_str>	Specify a descriptive name for the BGP neighbor interface.	Null.
keep-alive-timer <seconds_integer>	The frequency (in seconds) that a keepalive message is sent from the FortiGate unit to the BGP neighbor. This value overrides the global keep-alive-timer value (see "keepalive-timer <seconds_integer>" on page 288). The range is from 0 to 65 535.	-1 (not set)
maximum-prefix <prefix_integer>	Set the maximum number of NLRI prefixes to accept from the BGP neighbor. When the maximum is reached, the FortiGate unit disconnects the BGP neighbor. The range is from 1 to 4 294 967 295. Changing this value on the FortiGate unit does not disconnect the BGP neighbor. However, if the neighbor goes down because it reaches the maximum number of prefixes and you increase the maximum-prefix value afterward, the neighbor will be reset.	unset
maximum-prefix6 <prefix_integer>	Set the maximum number of NLRI prefixes to accept from the IPv6 BGP neighbor. When the maximum is reached, the FortiGate unit disconnects the BGP neighbor. The range is from 1 to 4 294 967 295. Changing this value on the FortiGate unit does not disconnect the BGP neighbor. However, if the neighbor goes down because it reaches the maximum number of prefixes and you increase the maximum-prefix value afterward, the neighbor will be reset.	unset
maximum-prefix-threshold <percentage_integer>	This field is available when maximum-prefix is set. Specify the threshold (as a percentage) that must be exceeded before a warning message about the maximum number of NLRI prefixes is displayed. The range is from 1 to 100.	75
maximum-prefix-threshold6 <percentage_integer>	This field is available when maximum-prefix6 is set. Specify the threshold (as a percentage) that must be exceeded before a warning message about the maximum number of NLRI prefixes is displayed. The range is from 1 to 100.	75
maximum-prefix-warning-only {enable | disable}	This field is available when maximum-prefix is set. Enable or disable the display of a warning when the maximum-prefix-threshold has been reached.	disable
maximum-prefix-warning-only6 {enable | disable}	This field is available when maximum-prefix6 is set. Enable or disable the display of a warning when the maximum-prefix-threshold6 has been reached.	disable
next-hop-self {enable | disable}	Enable or disable advertising of the FortiGate unit's IP address (instead of the neighbor's IP address) in the NEXT_HOP information that is sent to IBGP peers.	disable
next-hop-self6 {enable | disable}	Enable or disable advertising of the FortiGate unit's IP address (instead of the neighbor's IP address) in the NEXT_HOP information that is sent to IBGP peers.	disable
override-capability {enable | disable}	Enable or disable IPv6 addressing for a BGP neighbor that does not support capability negotiation.	disable

Variable	Description	Default
`passive {enable | disable}`	Enable or disable the sending of Open messages to BGP neighbors.	`disable`
`password <string>`	Enter password used in MD5 authentication to protect BGP sessions. (RFC 2385)	`Null.`
`prefix-list-in <prefix-list-name_str>`	Limit route updates from a BGP neighbor based on the Network Layer Reachability Information (NLRI) in the specified prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See "router prefix-list, prefix-list6" on page 337.	`Null.`
`prefix-list-in6 <prefix-list-name_str>`	Limit route updates from an IPv6 BGP neighbor based on the Network Layer Reachability Information (NLRI) in the specified prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See "router prefix-list, prefix-list6" on page 337.	`Null`
`prefix-list-out <prefix-list-name_str>`	Limit route updates to a BGP neighbor based on the NLRI in the specified prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See "router prefix-list, prefix-list6" on page 337.	`Null.`
`prefix-list-out6 <prefix-list-name_str>`	Limit route updates to an IPv6 BGP neighbor based on the NLRI in the specified prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See "router prefix-list, prefix-list6" on page 337.	`Null`
`remote-as <id_integer>`	Adds a BGP neighbor to the FortiGate unit configuration and sets the AS number of the neighbor. The range is from 1 to 65 535. If the number is identical to the FortiGate unit AS number, the FortiGate unit communicates with the neighbor using internal BGP (IBGP). Otherwise, the neighbor is an external peer and the FortiGate unit uses EBGP to communicate with the neighbor.	unset
`remove-private-as {enable | disable}`	Remove the private AS numbers from outbound updates to the BGP neighbor.	`disable`
`remove-private-as6 {enable | disable}`	Remove the private AS numbers from outbound updates to the IPv6 BGP neighbor.	`disable`
`restart_time <seconds_integer>`	Sets the time until a restart happens. The time until the restart can be from 0 to 3600 seconds.	0
`retain-stale-time <seconds_integer>`	This field is available when `capability-graceful-restart` is set to `enable`. Specify the time (in seconds) that stale routes to the BGP neighbor will be retained. The range is from 1 to 65 535. A value of 0 disables this feature.	`0`
`route-map-in <routemap-name_str>`	Limit route updates or change the attributes of route updates from the BGP neighbor according to the specified route map. You must create the route-map before it can be selected here. See "route-map" on page 354 and "Using route maps with BGP" on page 356.	`Null.`
`route-map-in6 <routemap-name_str>`	Limit route updates or change the attributes of route updates from the IPv6 BGP neighbor according to the specified route map. You must create the route-map before it can be selected here.	`Null`
`route-map-out <routemap-name_str>`	Limit route updates or change the attributes of route updates to the BGP neighbor according to the specified route map. You must create the route-map before it can be selected here. See "route-map" on page 354 and "Using route maps with BGP" on page 356.	`Null.`

Variable	Description	Default
`route-map-out6 <routemap-name_str>`	Limit route updates or change the attributes of route updates to the IPv6 BGP neighbor according to the specified route map. You must create the route-map before it can be selected here.	`Null`
`route-reflector-client {enable | disable}`	This field is available when `remote-as` is identical to the FortiGate unit AS number (see "as <local_as_id>" on page 286). Enable or disable the operation of the FortiGate unit as a route reflector and identify the BGP neighbor as a route-reflector client. Inbound routes for route reflectors can change the `next-hop, local-preference, med, and as-path` attributes of IBGP routes for local route selection, while outbound IBGP routes do not take into effect these attributes.	`disable`
`route-reflector-client6 {enable | disable}`	This field is available when `remote-as` is identical to the FortiGate unit AS number. Enable or disable the operation of the FortiGate unit as a route reflector and identify the BGP neighbor as a route-reflector client. Inbound routes for route reflectors can change the `next-hop, local-preference, med, and as-path` attributes of IBGP routes for local route selection, while outbound IBGP routes do not take into effect these attributes.	`disable`
`route-server-client {enable | disable}`	Enable or disable the recognition of the BGP neighbor as route-server client.	`disable`
`route-server-client6 {enable | disable}`	Enable or disable the recognition of the IPv6 BGP neighbor as route-server client.	`disable`
`send-community {both | disable | extended | standard}`	Enable sending the COMMUNITY attribute to the BGP neighbor. Choose one of: **`standard`** — advertise standard capabilities. **`extended`** — advertise extended capabilities. **`both`** — advertise extended and standard capabilities. **`disable`** — disable the advertising of the COMMUNITY attribute.	`both`
`send-community6 {both | disable | extended | standard}`	Enable sending the COMMUNITY attribute to the IPv6 BGP neighbor. Choose one of: **`standard`** — advertise standard capabilities **`extended`** — advertise extended capabilities **`both`** — advertise extended and standard capabilities **`disable`** — disable the advertising of the COMMUNITY attribute.	`both`
`shutdown {enable | disable}`	Administratively enable or disable the BGP neighbor.	`disable`
`soft-reconfiguration {enable | disable}`	Enable or disable the FortiGate unit to store unmodified updates from the BGP neighbor to support inbound soft-reconfiguration.	`disable`
`soft-reconfiguration6 {enable | disable}`	Enable or disable the FortiGate unit to store unmodified updates from the IPv6 BGP neighbor to support inbound soft-reconfiguration.	`disable`
`strict-capability-match {enable | disable}`	Enable or disable strict-capability negotiation matching with the BGP neighbor.	`disable`
`unsuppress-map <route-map-name_str>`	Specify the name of the route-map to selectively unsuppress suppressed routes. You must create the route-map before it can be selected here. See "route-map" on page 354 and "Using route maps with BGP" on page 356.	`Null.`

Variable	Description	Default
unsuppress-map6 <route-map-name_str>	Specify the name of the route-map to selectively unsuppress suppressed IPv6 routes. You must create the route-map before it can be selected here.	Null
update-source <interface-name_str>	Specify the name of the local FortiGate unit interface to use for TCP connections to neighbors. The IP address of the interface will be used as the source address for outgoing updates.	Null.
weight <weight_integer>	Apply a weight value to all routes learned from a neighbor. A higher number signifies a greater preference. The range is from 0 to 65 535.	unset

Example

This example shows how to set the AS number of a BGP neighbor at IP address 10.10.10.167 and enter a descriptive name for the configuration.

```
config router bgp
  config neighbor
    edit 10.10.10.167
      set remote-as 2879
      set description BGP_neighbor_Site1
    end
  end
```

config network

config network6

Use this subcommand to set or unset BGP network configuration parameters. The subcommand is used to advertise a BGP network (that is, an IP prefix) — you specify the IP addresses making up the local BGP network. Use `config network6` for IPv6 routing.

When you enable the `network-import-check` attribute on the FortiGate unit (see "network-import-check {enable | disable}" on page 288) and you specify a BGP network prefix through the `config network` command, the FortiGate unit searches its routing table for a matching entry. If an exact match is found, the prefix is advertised. A route-map can optionally be used to modify the attributes of routes before they are advertised.

Note: The `prefix` field is required. All other fields are optional.

Variable	Description	Default
edit <network_id>	Enter an ID number for the entry. The number must be an integer.	No default.
backdoor {enable | disable}	Enable or disable the route as a backdoor, which causes an administrative distance of 200 to be assigned to the route. Backdoor routes are not advertised to EBGP peers.	disable
prefix <address_ipv4mask>	Enter the IP address and netmask that identifies the BGP network to advertise.	0.0.0.0 0.0.0.0
prefix6 <address_ipv6mask>	Enter the IP address and netmask that identifies the BGP network to advertise.	::/0
route-map <routemap-name_str>	Specify the name of the route-map that will be used to modify the attributes of the route before it is advertised. You must create the route-map before it can be selected here. See "route-map" on page 354 and "Using route maps with BGP" on page 356.	Null.

Example

This example defines a BGP network at IP address `10.0.0.0/8`. A route map named `BGP_rmap1` is used to modify the attributes of the local BGP routes before they are advertised.

```
config router bgp
  config network
    edit 1
      set prefix 10.0.0.0/8
      set route-map BGP_rmap1
    end
  end

config router route-map
  edit BGP_rmap1
    config rule
    edit 1
      set set-community no-export
    end
  end
```

config redistribute

config redistribute6

Use this subcommand to set or unset BGP redistribution table parameters. Use `config redistribute6` for IPv6 routing. You can enable BGP to provide connectivity between connected, static, RIP, and/or OSPF routes. BGP redistributes the routes from one protocol to another. When a large internetwork is divided into multiple routing domains, use the subcommand to redistribute routes to the various domains. As an alternative, you can use the `config network` subcommand to advertise a prefix to the BGP network (see "config network" on page 296).

The BGP redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- `connected` — Redistribute routes learned from a direct connection to the destination network.
- `static` — Redistribute the static routes defined in the FortiGate unit routing table.
- `rip` — Redistribute routes learned from RIP.
- `ospf` — Redistribute routes learned from OSPF.

When you enter the subcommand, end the command with one of the four static entry names (that is, `config redistribute {connected | static | rip | ospf}`).

Note: The `status` and `route-map` fields are optional.

Variable	Description	Default
`status {enable | disable}`	Enable or disable the redistribution of connected, static, RIP, or OSPF routes.	`disable`
`route-map <route-map-name_str>`	Specify the name of the route map that identifies the routes to redistribute. You must create the route map before it can be selected here. See "route-map" on page 354 and "Using route maps with BGP" on page 356. If a route map is not specified, all routes are redistributed to BGP.	`Null.`

Example

The following example changes the `status` and `route-map` fields of the `connected` entry.

```
config router bgp
  config redistribute connected
    set status enable
    set route-map rmap1
  end
end
```

History

FortiOS v3.0	New.
FortiOS v3.0 MR6	Changed `ebgp-multihop` to `ebgp-enforced-mutlihop`. Changed `config neighbor capability-orf` field from `disable` to `none`.
FortiOS v3.0 MR7	Added `password` to `config neighbor`. Changed keep-alive-timer to keepalive-timer. Default time for holdtime-timer changed from 240 to 180.
FortiOS v4.0 MR1	Added `config aggregate-address6` subcommand with `prefix6` field. Added `config network6`, `config redistribute6` subcommands. In `config neighbor` subcommand, added `allowas-in6`, `allowas-in-enable6`, `attribute-unchanged6`, `capability-default-originate6`, `capability-graceful-restart6`, `capability-orf6`, `default-originate-route-map`, `default-originate-route-map6`, `distribute-list-in6`, `distribute-list-out6`, `filter-list-in6`, `filter-list-out6`, `maximum-prefix6`, `maximum-prefix-threshold6`, `maximum-prefix-warning-only6`, `next-hop-self6`, `prefix-list-in6`, `prefix-list-out6`, `remove-private-as6`, `route-map-in6`, `route-map-out6`, `route-reflector-client6`, `route-server-client6`, `send-community6`, `soft-reconfiguration6`, `unsuppress-map6`.

Related topics

- router aspath-list
- router community-list
- router route-map
- Using route maps with BGP
- router key-chain

community-list

Use this command to identify BGP routes according to their COMMUNITY attributes (see RFC 1997). Each entry in the community list defines a rule for matching and selecting routes based on the setting of the COMMUNITY attribute. The default rule in a community list (which the FortiGate unit applies last) denies the matching of all routes.

You add a route to a community by setting its COMMUNITY attribute. A route can belong to more than one community. A route may be added to a community because it has something in common with the other routes in the group (for example, the attribute could identify all routes to satellite offices).

When the COMMUNITY attribute is set, the FortiGate unit can select routes based on their COMMUNITY attribute values.

Syntax

```
config router community-list
  edit <community_name>
  set type {standard | expanded}
    config rule
      edit <community_rule_id>
        set action {deny | permit}
        set match <criteria>
        set regexp <regular_expression>
      end
    end
```

Note: The `action` field is required. All other fields are optional.

Variable	Description	Default
`edit <community_name>`	Enter a name for the community list.	No default.
`type {standard | expanded}`	Specify the type of community to match. If you select `expanded`, you must also specify a `config rule regexp` value. See “regexp <regular_expression>” on page 300.	standard
`config rule variables`		
`edit <community_rule_id>`	Enter an entry number for the rule. The number must be an integer.	No default.
`action {deny | permit}`	Deny or permit operations on a route based on the value of the route’s COMMUNITY attribute.	No default.

Variable	Description	Default
match <criteria>	This field is available when set type is set to standard. Specify the criteria for matching a reserved community. • Use decimal notation to match one or more COMMUNITY attributes having the syntax AA:NN, where AA represents an AS, and NN is the community identifier. Delimit complex expressions with double-quotation marks (for example, "123:234 345:456"). • To match all routes in the Internet community, type internet. • To match all routes in the LOCAL_AS community, type local-AS. Matched routes are not advertised locally. • To select all routes in the NO_ADVERTISE community, type no-advertise. Matched routes are not advertised. • To select all routes in the NO_EXPORT community, type no-export. Matched routes are not advertised to EBGP peers. If a confederation is configured, the routes are advertised within the confederation.	Null.
regexp <regular_expression>	This field is available when set type is set to expanded. Specify an ordered list of COMMUNITY attributes as a regular expression. The value or values are used to match a community. Delimit a complex regular_expression value using double-quotation marks.	Null.

Example

This example creates a community list named Satellite_offices. The list permits operations on BGP routes whose COMMUNITY attribute is set to no-advertise.

```
config router community-list
  edit Satellite_offices
    set type standard
    config rule
      edit 1
        set action permit
        set match no-advertise
      end
  end
```

The next example creates a community list named ext_community. The list permits operations on BGP routes whose COMMUNITY attribute has the number 3 in the second part of the first instance and the number 86 in the second part of the second instance. For example, the community list could match routes having the following COMMUNITY attribute values: "100:3 500:86 300:800", "1:3 4:86", or "69:3 69:86 69:69 70:800 600:333").

```
config router community-list
  edit ext_community
    set type expanded
    config rule
      edit 1
        set action permit
        set regexp ".*:3 .*:86"
      end
  end
```

History

FortiOS v3.0 New.

Related topics

- router aspath-list
- router bgp
- router Using route maps with BGP
- router key-chain

key-chain

Use this command to manage RIP version 2 authentication keys. You can add, edit or delete keys identified by the specified key number.

RIP version 2 uses authentication keys to ensure that the routing information exchanged between routers is reliable. For authentication to work, both the sending and receiving routers must be set to use authentication, and must be configured with the same keys.

A key chain is a list of one or more keys and the send and receive lifetimes for each key. Keys are used for authenticating routing packets only during the specified lifetimes. The FortiGate unit migrates from one key to the next according to the scheduled send and receive lifetimes. The sending and receiving routers should have their system dates and times synchronized, but overlapping the key lifetimes ensures that a key is always available even if there is some difference in the system times. For how to to ensure that the FortiGate unit system date and time are correct, see “config system global” on page 243 .

Syntax

```
config router key-chain
  edit <key_chain_name>
    config key
      edit <key_id>
        set accept-lifetime <start> <end>
        set key-string <password>
        set send-lifetime <start> <end>
      end
  end
```

Note: The `accept-lifetime`, `key-string`, and `send-lifetime` fields are required.

Variable	Description	Default
`edit <key_chain_name>`	Enter a name for the key chain list.	No default.
config key variables		
`edit <key_id>`	Enter an ID number for the key entry. The number must be an integer.	No default.
`accept-lifetime <start> <end>`	Set the time period during which the key can be received. The `start` time has the syntax `hh:mm:ss day month year`. The `end` time provides a choice of three settings: **`hh:mm:ss day month year`** **`<integer>`** — a duration from 1 to 2147483646 seconds **`infinite`** — for a key that never expires The valid settings for **`hh:mm:ss day month year`** are: **`hh`** — 0 to 23 **`mm`** — 0 to 59 **`ss`** — 0 to 59 **`day`** — 1 to 31 **`month`** — 1 to 12 **`year`** — 1993 to 2035 **Note:** A single digit will be accepted for **`hh`**, **`mm`**, **`ss`**, **`day`**, or **`month`** fields.	No default.

Variable	Description	Default
`key-string <password>`	The `<password_str>` can be up to 35 characters long.	No default.
`send-lifetime <start> <end>`	Set the time period during which the key can be sent. The `start` time has the syntax `hh:mm:ss day month year`. The `end` time provides a choice of three settings: **`hh:mm:ss day month year`** **`<integer>`** — a duration from 1 to 2147483646 seconds **`infinite`** — for a key that never expires The valid settings for **`hh:mm:ss day month year`** are: **`hh`** — 0 to 23 **`mm`** — 0 to 59 **`ss`** — 0 to 59 **`day`** — 1 to 31 **`month`** — 1 to 12 **`year`** — 1993 to 2035 **Note:** A single digit will be accepted for **`hh`**, **`mm`**, **`ss`**, **`day`**, or **`month`** fields.	No default.

Example

This example shows how to add a key chain named `test1` with three keys. The first two keys each have send and receive lifetimes of 13 hours, and the 3rd key has send and receive lifetimes that never expire.

```
config router key-chain
  edit test1
    config key
      edit 1
        set accept-lifetime 10:00:00 1 6 2004 46800
        set send-lifetime 10:00:00 1 6 2004 46800
        set key-string 1a2b2c4d5e6f7g8h
      next
      edit 2
        set accept-lifetime 22:00:00 1 6 2004 46800
        set send-lifetime 22:00:00 1 6 2004 46800
        set key-string 9i1j2k3l4m5n6o7p
      next
      edit 3
        set accept-lifetime 10:00:00 2 6 2004 infinite
        set send-lifetime 10:00:00 2 6 2004 infinite
        set key-string 123abc456def789g
      end
  end
```

History

FortiOS v2.80 New.

Related topics

- router rip
- system global

multicast

A FortiGate unit can operate as a Protocol Independent Multicast (PIM) version 2 router. FortiGate units support PIM sparse mode (RFC 4601) and PIM dense mode (RFC 3973) and can service multicast servers or receivers on the network segment to which a FortiGate unit interface is connected. Multicast routing is not supported in Transparent mode (TP mode).

Note: To support PIM communications, the sending/receiving applications and all connecting PIM routers in between must be enabled with PIM version 2. PIM can use static routes, RIP, OSPF, or BGP to forward multicast packets to their destinations. To enable source-to-destination packet delivery, either sparse mode or dense mode must be enabled on the PIM-router interfaces. Sparse mode routers cannot send multicast messages to dense mode routers. In addition, if a FortiGate unit is located between a source and a PIM router, two PIM routers, or is connected directly to a receiver, you must create a firewall policy manually to pass encapsulated (multicast) packets or decapsulated data (IP traffic) between the source and destination.

A PIM domain is a logical area comprising a number of contiguous networks. The domain contains at least one Boot Strap Router (BSR), and if sparse mode is enabled, a number of Rendezvous Points (RPs) and Designated Routers (DRs). When PIM is enabled on a FortiGate unit, the FortiGate unit can perform any of these functions at any time as configured.

Sparse mode

Initially, all candidate BSRs in a PIM domain exchange bootstrap messages to select one BSR to which each RP sends the multicast address or addresses of the multicast group(s) that it can service. The selected BSR chooses one RP per multicast group and makes this information available to all of the PIM routers in the domain through bootstrap messages. PIM routers use the information to build packet distribution trees, which map each multicast group to a specific RP. Packet distribution trees may also contain information about the sources and receivers associated with particular multicast groups.

Note: When a FortiGate unit interface is configured as a multicast interface, sparse mode is enabled on it by default to ensure that distribution trees are not built unless at least one downstream receiver requests multicast traffic from a specific source. If the sources of multicast traffic and their receivers are close to each other and the PIM domain contains a dense population of active receivers, you may choose to enable dense mode throughout the PIM domain instead.

An RP represents the root of a non-source-specific distribution tree to a multicast group. By joining and pruning the information contained in distribution trees, a single stream of multicast packets (for example, a video feed) originating from the source can be forwarded to a certain RP to reach a multicast destination.

Each PIM router maintains a Multicast Routing Information Base (MRIB) that determines to which neighboring PIM router join and prune messages are sent. An MRIB contains reverse-path information that reveals the path of a multicast packet from its source to the PIM router that maintains the MRIB.

To send multicast traffic, a server application sends IP traffic to a multicast group address. The locally elected DR registers the sender with the RP that is associated with the target multicast group. The RP uses its MRIB to forward a single stream of IP packets from the source to the members of the multicast group. The IP packets are replicated only when necessary to distribute the data to branches of the RP's distribution tree.

To receive multicast traffic, a client application can use Internet Group Management Protocol (IGMP) version 1 (RFC 1112), 2 (RFC 2236), or 3 (RFC 3376) control messages to request the traffic for a particular multicast group. The locally elected DR receives the request and adds the host to the multicast group that is associated with the connected network segment by sending a join message towards the RP for the group. Afterward, the DR queries the hosts on the connected network segment continually to determine whether the hosts are active. When the DR no longer receives confirmation that at least one member of the multicast group is still active, the DR sends a prune message towards the RP for the group.

Dense mode

The packet organization used in sparse mode is also used in dense mode. When a multicast source begins to send IP traffic and dense mode is enabled, the closest PIM router registers the IP traffic from the multicast source (S) and forwards multicast packets to the multicast group address (G). All PIM routers initially broadcast the multicast packets throughout the PIM domain to ensure that all receivers that have requested traffic for multicast group address G can access the information if needed.

To forward multicast packets to specific destinations afterward, the PIM routers build distribution trees based on the information in multicast packets. Upstream PIM routers depend on prune/graft messages from downstream PIM routers to determine if receivers are actually present on directly connected network segments. The PIM routers exchange state refresh messages to update their distribution trees. FortiGate units store this state information in a Tree Information Base (TIB), which is used to build a multicast forwarding table. The information in the multicast forwarding table determines whether packets are forwarded downstream. The forwarding table is updated whenever the TIB is modified.

PIM routers receive data streams every few minutes and update their forwarding tables using the source (S) and multicast group (G) information in the data stream. Superfluous multicast traffic is stopped by PIM routers that do not have downstream receivers—PIM routers that do not manage multicast groups send prune messages to the upstream PIM routers. When a receiver requests traffic for multicast address G, the closest PIM router sends a graft message upstream to begin receiving multicast packets.

For more information on Multicast routing, see the FortiGate Multicast Technical Note.

Syntax

```
config router multicast
  set igmp-state-limit <limit_integer>
  set multicast-routing {enable | disable}
  set route-limit <limit_integer>
  set route-threshold <threshold_integer>
  config interface
    edit <interface_name>
      set cisco-exclude-genid {enable | disable}
      set dr-priority <priority_integer>
      set hello-holdtime <holdtime_integer>
      set hello-interval <hello_integer>
      set neighbour-filter <access_list_name>
      set passive {enable | disable}
      set pim-mode {sparse-mode | dense-mode}
      set propagation-delay <delay_integer>
      set rp-candidate {enable | disable}
      set rp-candidate-group <access_list_name>
      set rp-candidate-interval <interval_integer>
      set rp-candidate-priority <priority_integer>
      set state-refresh-interval <refresh_integer>
      set ttl-threshold <ttl_integer>
    end
    config join-group
      edit address <address_ipv4>
    end
    config igmp
      set access-group <access_list_name>
      set immediate-leave-group <access_list_name>
      set last-member-query-count <count_integer>
      set last-member-query-interval <interval_integer>
      set query-interval <interval_integer>
```

```
    set query-max-response-time <time_integer>
    set query-timeout <timeout_integer>
    set router-alert-check { enable | disable }
    set version {1 | 2 | 3}
  end
end
config pim-sm-global
  set accept-register-list <access_list_name>
  set bsr-allow-quick-refresh {enable | disable}
  set bsr-candidate {enable | disable}
  set bsr-priority <priority_integer>
  set bsr-interface <interface_name>
  set bsr-hash <hash_integer>
  set cisco-register-checksum {enable | disable}
  set cisco-register-checksum-group <access_list_name>
  set cisco-crp-prefix {enable | disable}
  set cisco-ignore-rp-set-priority {enable | disable}
  set message-interval <interval_integer>
  set register-rate-limit <rate_integer>
  set register-rp-reachability {enable | disable}
  set register-source {disable | interface | ip-address}
  set register-source-interface <interface_name>
  set register-source-ip <address_ipv4>
  set register-suppression <suppress_integer>
  set rp-register-keepalive <keepalive_integer>
  set spt-threshold {enable | disable}
  set spt-threshold-group <access_list_name>
  set ssm {enable | disable}
  set ssm-range <access_list_name>
  config rp-address
    edit <rp_id>
      set ip-address <address_ipv4>
      set group <access_list_name>
    end
end
```

config router multicast

You can configure a FortiGate unit to support PIM using the `config router multicast` CLI command. When PIM is enabled, the FortiGate unit allocates memory to manage mapping information. The FortiGate unit communicates with neighboring PIM routers to acquire mapping information and if required, processes the multicast traffic associated with specific multicast groups.

Note: The end-user multicast client-server applications must be installed and configured to initiate Internet connections and handle broadband content such as audio/video information.

Client applications send multicast data by registering IP traffic with a PIM-enabled router. An end-user could type in a class D multicast group address, an alias for the multicast group address, or a call-conference number to initiate the session.

Rather than sending multiple copies of generated IP traffic to more than one specific IP destination address, PIM-enabled routers encapsulate the data and use the one multicast group address to forward multicast packets to multiple destinations. Because one destination address is used, a single stream of data can be sent. Client applications receive multicast data by requesting that the traffic destined for a certain multicast group address be delivered to them— end-users may use phone books, a menu of ongoing or future sessions, or some other method through a user interface to select the address of interest.

A class D address in the 224.0.0.0 to 239.255.255.255 range may be used as a multicast group address, subject to the rules assigned by the Internet Assigned Numbers Authority (IANA). All class D addresses must be assigned in advance. Because there is no way to determine in advance if a certain multicast group address is in use, collisions may occur (to resolve this problem, end-users may switch to a different multicast address).

To configure a PIM domain

1. If you will be using sparse mode, determine appropriate paths for multicast packets.
2. Make a note of the interfaces that will be PIM-enabled. These interfaces may run a unicast routing protocol.
3. If you will be using sparse mode and want multicast packets to be handled by specific (static) RPs, record the IP addresses of the PIM-enabled interfaces on those RPs.
4. Enable PIM version 2 on all participating routers between the source and receivers. On FortiGate units, use the `config router multicast` command to set global operating parameters.
5. Configure the PIM routers that have good connections throughout the PIM domain to be candidate BSRs.
6. If sparse mode is enabled, configure one or more of the PIM routers to be candidate RPs.
7. If required, adjust the default settings of PIM-enabled interface(s).

Note: All fields are optional.

Variable	Description	Default
`igmp-state-limit <limit_integer>`	If memory consumption is an issue, specify a limit on the number of IGMP states (multicast memberships) that the FortiGate unit will store. This value represents the maximum combined number of IGMP states (multicast memberships) that can be handled by all interfaces. Traffic associated with excess IGMP membership reports is not delivered. The range is from `96` to `64 000`.	`3200`
`multicast-routing {enable | disable}`	Enable or disable PIM routing.	`disable`
`route-limit <limit_integer>`	If memory consumption is an issue, set a limit on the number of multicast routes that can be added to the FortiGate unit routing table. The range is from `1` to `2 147 483 674`.	`2147483674`
`route-threshold <threshold_integer>`	Specify the number of multicast routes that can be added to the FortiGate unit's routing table before a warning message is displayed. The `route-threshold` value must be lower than the `route-limit` value. The range is from `1` to `2 147 483 674`.	`2147483674`

config interface

Use this subcommand to change interface-related PIM settings, including the mode of operation (sparse or dense). Global settings do not override interface-specific settings.

Note: All fields are optional.

Variable	Description	Default
`edit <interface_name>`	Enter the name of the FortiGate unit interface on which to enable PIM protocols.	No default.
`cisco-exclude-genid {enable | disable}`	This field applies only when `pim-mode` is `sparse-mode`. Enable or disable including a generation ID in hello messages sent to neighboring PIM routers. A GenID value may be included for compatibility with older Cisco IOS routers.	disable
`dr-priority <priority_integer>`	This field applies only when `pim-mode` is `sparse-mode`. Assign a priority to FortiGate unit Designated Router (DR) candidacy. The range is from 1 to 4 294 967 294. The value is compared to that of other DR interfaces connected to the same network segment, and the router having the highest DR priority is selected to be the DR. If two DR priority values are the same, the interface having the highest IP address is selected.	`1`
`hello-holdtime <holdtime_integer>`	Specify the amount of time (in seconds) that a PIM neighbor may consider the information in a hello message to be valid. The range is from 1 to 65 535. If the `hello-interval` attribute is modified and the `hello-holdtime` attribute has never been set explicitly, the `hello-holdtime` attribute is automatically set to 3.5 x `hello-interval`.	`105`
`hello-interval <hello_integer>`	Set the amount of time (in seconds) that the FortiGate unit waits between sending hello messages to neighboring PIM routers. The range is from 1 to 65 535. Changing the `hello-interval` attribute may automatically update the `hello-holdtime` attribute .	`30`
`neighbour-filter <access_list_name>`	Establish or terminate adjacency with PIM neighbors having the IP addresses given in the specified access list. For more information on access lists, see “access-list, access-list6” on page 276.	`Null.`
`passive {enable | disable}`	Enable or disable PIM communications on the interface without affecting IGMP communications.	`disable`
`pim-mode {sparse-mode | dense-mode}`	Select the PIM mode of operation. Choose one of: **`sparse-mode`** — manage PIM packets through distribution trees and multicast groups. **`dense-mode`** — enable multicast flooding.	`sparse-mode`
`propagation-delay <delay_integer>`	This field is available when `pim-mode` is set to `dense-mode`. Specify the amount of time (in milliseconds) that the FortiGate unit waits to send prune-override messages. The range is from 100 to 5 000.	500
`rp-candidate {enable | disable}`	This field is available when `pim-mode` is set to `sparse-mode`. Enable or disable the FortiGate unit interface to offer Rendezvous Point (RP) services.	disable
`rp-candidate-group <access_list_name>`	RP candidacy is advertised to certain multicast groups. These groups are based on the multicast group prefixes given in the specified access list. For more information on access lists, see “access-list, access-list6” on page 276. This field is available when `rp-candidate` is set to `enable` and `pim-mode` is set to `sparse-mode`.	`Null.`

Variable	Description	Default
rp-candidate-interval <interval_integer>	This field is available when rp-candidate is set to enable and pim-mode is set to sparse-mode. Set the amount of time (in seconds) that the FortiGate unit waits between sending RP announcement messages. The range is from 1 to 16 383.	60
rp-candidate-priority <priority_integer>	This field is available when rp-candidate is set to enable and pim-mode is set to sparse-mode. Assign a priority to FortiGate unit Rendezvous Point (RP) candidacy. The range is from 0 to 255. The BSR compares the value to that of other RP candidates that can service the same multicast group, and the router having the highest RP priority is selected to be the RP for that multicast group. If two RP priority values are the same, the RP candidate having the highest IP address on its RP interface is selected.	192
state-refresh-interval <refresh_integer>	This field is available when pim-mode is set to dense-mode. This attribute is used when the FortiGate unit is connected directly to the multicast source. Set the amount of time (in seconds) that the FortiGate unit waits between sending state-refresh messages. The range is from 1 to 100. When a state-refresh message is received by a downstream router, the prune state on the downstream router is refreshed.	60
ttl-threshold <ttl_integer>	Specify the minimum Time-To-Live (TTL) value (in hops) that an outbound multicast packet must have in order to be forwarded from this interface. The range is from 0 to 255. Specifying a high value (for example, 195) prevents PIM packets from being forwarded through the interface.	1
config join-group variables		
edit address <address_ipv4>	Cause the FortiGate unit interface to activate (IGMP join) the multicast group associated with the specified multicast group address.	No default.
config igmp variables		
access-group <access_list_name>	Specify which multicast groups that hosts on the connected network segment may join based on the multicast addresses given in the specified access list. For more information on access lists, see “access-list, access-list6” on page 276.	Null.
immediate-leave-group <access_list_name>	This field applies when version is set to 2 or 3. Configure a FortiGate unit DR to stop sending traffic and IGMP queries to receivers after receiving an IGMP version 2 group-leave message from any member of the multicast groups identified in the specified access list. For more information on access lists, see “access-list, access-list6” on page 276.	Null.
last-member-query-count <count_integer>	This field applies when version is set to 2 or 3. Specify the number of times that a FortiGate unit DR sends an IGMP query to the last member of a multicast group after receiving an IGMP version 2 group-leave message.	2
last-member-query-interval <interval_integer>	This field applies when version is set to 2 or 3. Set the amount of time (in milliseconds) that a FortiGate unit DR waits for the last member of a multicast group to respond to an IGMP query. The range is from 1000 to 25 500. If no response is received before the specified time expires and the FortiGate unit DR has already sent an IGMP query last-member-query-count times, the FortiGate unit DR removes the member from the group and sends a prune message to the associated RP.	1000
query-interval <interval_integer>	Set the amount of time (in seconds) that a FortiGate unit DR waits between sending IGMP queries to determine which members of a multicast group are active. The range is from 1 to 65 535.	125

Variable	Description	Default
query-max-response-time <time_integer>	Set the maximum amount of time (in seconds) that a FortiGate unit DR waits for a member of a multicast group to respond to an IGMP query. The range is from 1 to 25. If no response is received before the specified time expires, the FortiGate unit DR removes the member from the group.	10
query-timeout <timeout_integer>	Set the amount of time (in seconds) that must expire before a FortiGate unit begins sending IGMP queries to the multicast group that is managed through the interface. The range is from 60 to 300. A FortiGate unit begins sending IGMP queries if it does not receive regular IGMP queries from another DR through the interface.	255
router-alert-check { enable | disable }	Enable to require the Router Alert option in IGMP packets.	disabled
version {1 | 2 | 3}	Specify the version number of IGMP to run on the interface. The value can be 1, 2, or 3. The value must match the version used by all other PIM routers on the connected network segment.	3

config pim-sm-global

These global settings apply only to sparse mode PIM-enabled interfaces. Global PIM settings do not override interface-specific PIM settings.

If sparse mode is enabled, you can configure a DR to send multicast packets to a particular RP by specifying the IP address of the RP through the config rp-address variable. The IP address must be directly accessible to the DR. If multicast packets from more than one multicast group can pass through the same RP, you can use an access list to specify the associated multicast group addresses.

Note: To send multicast packets to a particular RP using the config rp-address subcommand, the ip-address field is required. All other fields are optional.

Variable	Description	Default
accept-register-list <access_list_name>	Cause a FortiGate unit RP to accept or deny register packets from the source IP addresses given in the specified access list. For more information on access lists, see “access-list, access-list6” on page 276.	Null.
bsr-allow-quick-refresh {enable | disable}	Enable or disable accepting BSR quick refresh packets from neighbors.	disable
bsr-candidate {enable | disable}	Enable or disable the FortiGate unit to offer its services as a Boot Strap Router (BSR) when required.	disable
bsr-priority <priority_integer>	This field is available when bsr-candidate is set to enable. Assign a priority to FortiGate unit BSR candidacy. The range is from 0 to 255. This value is compared to that of other BSR candidates and the candidate having the highest priority is selected to be the BSR. If two BSR priority values are the same, the BSR candidate having the highest IP address on its BSR interface is selected.	0
bsr-interface <interface_name>	This field is available when bsr-candidate is set to enable. Specify the name of the PIM-enabled interface through which the FortiGate unit may announce BSR candidacy.	Null.
bsr-hash <hash_integer>	This field is available when bsr-candidate is set to enable. Set the length of the mask (in bits) to apply to multicast group addresses in order to derive a single RP for one or more multicast groups. The range is from 0 to 32. For example, a value of 24 means that the first 24 bits of the group address are significant. All multicast groups having the same seed hash belong to the same RP.	10

Variable	Description	Default
`cisco-crp-prefix {enable | disable}`	Enable or disable a FortiGate unit RP that has a group prefix number of 0 to communicate with a Cisco BSR. You may choose to enable the attribute if required for compatibility with older Cisco BSRs.	disable
`cisco-ignore-rp-set-priority {enable | disable}`	Enable or disable a FortiGate unit BSR to recognize Cisco RP-SET priority values when deriving a single RP for one or more multicast groups. You may choose to enable the attribute if required for compatibility with older Cisco RPs.	disable
`cisco-register-checksum {enable | disable}`	Enable or disable performing a register checksum on entire PIM packets. A register checksum is performed on the header only by default. You may choose to enable register checksums on the whole packet for compatibility with older Cisco IOS routers.	disable
`cisco-register-checksum-group <access_list_name>`	This field is available when `cisco-register-checksum` is set to `enable`. Identify on which PIM packets to perform a whole-packet register checksum based on the multicast group addresses in the specified access list. For more information on access lists, see "access-list, access-list6" on page 276. You may choose to register checksums on entire PIM packets for compatibility with older Cisco IOS routers.	`Null.`
`message-interval <interval_integer>`	Set the amount of time (in seconds) that the FortiGate unit waits between sending periodic PIM join/prune messages (sparse mode) or prune messages (dense mode). The value must be identical to the message interval value set on all other PIM routers in the PIM domain. The range is from 1 to 65 535.	`60`
`register-rate-limit <rate_integer>`	Set the maximum number of register messages per (S,G) per second that a FortiGate unit DR can send for each PIM entry in the routing table. The range is from `0` to `65 535`, where `0` means an unlimited number of register messages per second.	0
`register-rp-reachability {enable | disable}`	Enable or disable a FortiGate unit DR to check if an RP is accessible prior to sending register messages.	`enable`
`register-source {disable | interface | ip-address}`	If the FortiGate unit acts as a DR, enable or disable changing the IP source address of outbound register packets to one of the following IP addresses. The IP address must be accessible to the RP so that the RP can respond to the IP address with a Register-Stop message. Choose one of: **`disable`** — retain the IP address of the FortiGate unit DR interface that faces the RP. **`interface`** — change the IP source address of a register packet to the IP address of a particular FortiGate unit interface. The `register-source-interface` attribute specifies the interface name. **`ip-address`** — change the IP source address of a register packet to a particular IP address. The `register-source-ip` attribute specifies the IP address.	`ip-address`
`register-source-interface <interface_name>`	Enter the name of the FortiGate unit interface. This field is only available when `register-source` is set to `interface`.	`Null.`
`register-source-ip <address_ipv4>`	This field is available when `register-source` is set to `address`. Enter the IP source address to include in the register message.	`0.0.0.0`
`register-suppression <suppress_integer>`	Enter the amount of time (in seconds) that a FortiGate unit DR waits to start sending data to an RP after receiving a Register-Stop message from the RP. The range is from 1 to 65 535.	60

Variable	Description	Default
rp-register-keepalive <keepalive_integer>	If the FortiGate unit acts as an RP, set the frequency (in seconds) with which the FortiGate unit sends keepalive messages to a DR. The range is from 1 to 65 535. The two routers exchange keepalive messages to maintain a link for as long as the source continues to generate traffic. If the register-suppression attribute is modified on the RP and the rp-register-keepalive attribute has never been set explicitly, the rp-register-keepalive attribute is set to (3 x register-suppression) + 5 automatically.	185
spt-threshold {enable | disable}	Enable or disable the FortiGate unit to build a Shortest Path Tree (SPT) for forwarding multicast packets.	enable
spt-threshold-group <access_list_name>	Build an SPT only for the multicast group addresses given in the specified access list. For more information on access lists, see “access-list, access-list6” on page 276. This field is only available when spt-threshold is set to enable.	Null.
ssm {enable | disable}	This field is available when the IGMP version is set to 3. Enable or disable Source Specific Multicast (SSM) interactions (see RFC 3569).	enable
ssm-range <access_list_name>	Enable SSM only for the multicast addresses given in the specified access list. For more information on access lists, see “access-list, access-list6” on page 276. By default, multicast addresses in the 232.0.0.0 to 232.255.255.255 (232/8) range are used to support SSM interactions. This field is only available when ssm is set to enable.\	Null.
config rp-address variables	Only used when pim-mode is sparse-mode.	
edit <rp_id>	Enter an ID number for the static RP address entry. The number must be an integer.	No default.
ip-address <address_ipv4>	Specify a static IP address for the RP.	0.0.0.0
group <access_list_name>	Configure a single static RP for the multicast group addresses given in the specified access list. For more information on access lists, see “access-list, access-list6” on page 276. If an RP for any of these group addresses is already known to the BSR, the static RP address is ignored and the RP known to the BSR is used instead.	Null.

Examples

This example shows how to enable a FortiGate unit to support PIM routing in sparse mode and enable BSR candidacy on the dmz interface:

```
config router multicast
  set multicast-routing enable
  config interface
    edit dmz
      set pim-mode sparse-mode
    end
  end
  config pim-sm-global
    set bsr-candidate enable
    set bsr-priority 1
    set bsr-interface dmz
    set bsr-hash 24
  end
```

This example shows how to enable RP candidacy on the `port1` interface for the multicast group addresses given through an access list named `multicast_port1`:

```
config router multicast
  set multicast-routing enable
  config interface
    edit port1
      set pim-mode sparse-mode
      set rp-candidate enable
      set rp-candidate-group multicast_port1
      set rp-candidate-priority 15
    end
  end
```

History

FortiOS v3.0 New.

Related topics

- router access-list, access-list6
- get router info multicast
- execute modem trigger

ospf

Use this command to configure Open Shortest Path First (OSPF) protocol settings on the FortiGate unit. More information on OSPF can be found in RFC 2328.

OSPF is a link state protocol capable of routing larger networks than the simpler distance vector RIP protocol. An OSPF autonomous system (AS) or routing domain is a group of areas connected to a backbone area. A router connected to more than one area is an area border router (ABR). Routing information is contained in a link state database. Routing information is communicated between routers using link state advertisements (LSAs).

Bi-directional Forwarding Detection (BFD) is a protocol used by BGP and OSPF. It is used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and if a timer runs out on a connection then that router is declared down. BFD then communicates this information to the routing protocol and the routing information is updated. BFD support can only be configured through the CLI.

Syntax

```
config router ospf
  set abr-type {cisco | ibm | shortcut | standard}
  set auto-cost-ref-bandwidth <mbps_integer>
  set bfd {enable | disable | global}
  set database-overflow {enable | disable}
  set database-overflow-max-lsas <lsas_integer>
  set database-overflow-time-to-recover <seconds_integer>
  set default-information-metric <metric_integer>
  set default-information-metric-type {1 | 2}
  set default-information-originate {always | disable | enable}
  set default-information-route-map <name_str>
  set default-metric <metric_integer>
  set distance <distance_integer>
  set distance-external <distance_integer>
  set distance-inter-area <distance_integer>
  set distance-intra-area <distance_integer>
  set distribute-list-in <access_list_name>
  set passive-interface <name_str>
  set restart-mode {graceful-restart | lls | none}
  set restart-period
  set rfc1583-compatible {enable | disable}
  set router-id <address_ipv4>
  set spf-timers <delay_integer> <hold_integer>
  config area
    edit <area_address_ipv4>
      set authentication {md5 | none | text}
      set default-cost <cost_integer>
      set nssa-default-information-originate {enable | disable}
      set nssa-default-information-originate-metric <metric>
      set nssa-default-information-originate-metric-type {1 | 2}
      set nssa-redistribution {enable | disable}
      set nssa-translator-role {always | candidate | never}
      set shortcut {default | disable | enable}
      set stub-type {no-summary | summary}
      set type {nssa | regular | stub}
      config filter-list
```

```
      edit <filter-list_id>
        set direction {in | out}
        set list <name_str>
      end
    config range
      edit <range_id>
        set advertise {enable | disable}
        set prefix <address_ipv4mask>
        set substitute <address_ipv4mask>
        set substitute-status {enable | disable}
    end
    config virtual-link
      edit <vlink_name>
        set authentication {md5 | none | text}
        set authentication-key <password_str>
        set dead-interval <seconds_integer>
        set hello-interval <seconds_integer>
        set md5-key <id_integer><key_str>
        set peer <address_ipv4>
        set retransmit-interval <seconds_integer>
        set transmit-delay <seconds_integer>
      end
    end
  config distribute-list
    edit <distribute-list_id>
      set access-list <name_str>
      set protocol {connected | rip | static}
    end
  end
  config neighbor
    edit <neighbor_id>
      set cost <cost_integer>
      set ip <address_ipv4>
      set poll-interval <seconds_integer>
      set priority <priority_integer>
    end
  end
  config network
    edit <network_id>
      set area <id-address_ipv4>
      set prefix <address_ipv4mask>
    end
  end
  config ospf-interface
    edit <ospf_interface_name>
      set authentication {md5 | none | text}
      set authentication-key <password_str>
      set
      set cost <cost_integer>
      set database-filter-out {enable | disable}
      set dead-interval <seconds_integer>
      set hello-interval <seconds_integer>
      set interface <name_str>
      set ip <address_ipv4>
```

```
        set md5-key <id_integer> <key_str>
        set mtu <mtu_integer>
        set mtu-ignore {enable | disable}
        set network-type <type>
        set priority <priority_integer>
        set resync-timeout <integer>
        set retransmit-interval <seconds_integer>
        set status {enable | disable}
        set transmit-delay <seconds_integer>
      end
    end
    config redistribute {bgp | connected | static | rip}
      set metric <metric_integer>
      set metric-type {1 | 2}
      set routemap <name_str>
      set status {enable | disable}
      set tag <tag_integer>
    end
    config summary-address
      edit <summary-address_id>
        set advertise {enable | disable}
        set prefix <address_ipv4mask>
        set tag <tag_integer>
      end
    end
  end
```

config router ospf

Use this command to set the router ID of the FortiGate unit. Additional configuration options are supported.

Note: The `router-id` field is required. All other fields are optional.

Variable	Description	Default
`abr-type {cisco | ibm | shortcut | standard}`	Specify the behavior of a FortiGate unit acting as an OSPF area border router (ABR) when it has multiple attached areas and has no backbone connection. Selecting the ABR type compatible with the routers on your network can reduce or eliminate the need for configuring and maintaining virtual links. For more information, see RFC 3509.	`standard`
`auto-cost-ref-bandwidth <mbps_integer>`	Enter the Mbits per second for the reference bandwidth. Values can range from 1 to 65535.	1000
`bfd {enable | disable | global}`	Select one of the Bidirectional Forwarding Detection (BFD) options for this interface. • enable - start BFD on this interface • disable - stop BFD on this interface • global - use the global settings instead of explicitly setting BFD per interface. For the global settings see "system bfd {enable | disable}" on page 518.	disable

Variable	Description	Default
database-overflow {enable | disable}	Enable or disable dynamically limiting link state database size under overflow conditions. Enable this command for FortiGate units on a network with routers that may not be able to maintain a complete link state database because of limited resources.	disable
database-overflow-max-lsas <lsas_integer>	If you have enabled database-overflow, set the limit for the number of external link state advertisements (LSAs) that the FortiGate unit can keep in its link state database before entering the overflow state. The lsas_integer must be the same on all routers attached to the OSPF area and the OSPF backbone. The valid range for lsas_integer is 0 to 4294967294.	10000
database-overflow-time-to-recover <seconds_integer>	Enter the time, in seconds, after which the FortiGate unit will attempt to leave the overflow state. If seconds_integer is set to 0, the FortiGate unit will not leave the overflow state until restarted. The valid range for seconds_integer is 0 to 65535.	300
default-information-metric <metric_integer>	Specify the metric for the default route set by the default-information-originate command. The valid range for metric_integer is 1 to 16777214.	10
default-information-metric-type {1 | 2}	Specify the OSPF external metric type for the default route set by the default-information-originate command.	2
default-information-originate {always | disable | enable}	Enter enable to advertise a default route into an OSPF routing domain. Use always to advertise a default route even if the FortiGate unit does not have a default route in its routing table.	disable
default-information-route-map <name_str>	If you have set default-information-originate to always, and there is no default route in the routing table, you can configure a route map to define the parameters that OSPF uses to advertise the default route.	Null.
default-metric <metric_integer>	Specify the default metric that OSPF should use for redistributed routes. The valid range for metric_integer is 1 to 16777214.	10
distance <distance_integer>	Configure the administrative distance for all OSPF routes. Using administrative distance you can specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. The valid range for distance_integer is 1 to 255.	110
distance-external <distance_integer>	Change the administrative distance of all external OSPF routes. The range is from 1 to 255.	110
distance-inter-area <distance_integer>	Change the administrative distance of all inter-area OSPF routes. The range is from 1 to 255.	110
distance-intra-area <distance_integer>	Change the administrative distance of all intra-area OSPF routes. The range is from 1 to 255.	110
distribute-list-in <access_list_name>	Limit route updates from the OSPF neighbor based on the Network Layer Reachability Information (NLRI) defined in the specified access list. You must create the access list before it can be selected here. See “access-list, access-list6” on page 276.	Null.
passive-interface <name_str>	OSPF routing information is not sent or received through the specified interface.	No default.

Variable	Description	Default
`restart-mode {graceful-restart | lls | none}`	Select the restart mode from: • graceful-restart - (also known as hitless restart) when FortiGate unit goes down it advertises to neighbors how long it will be down to reduce traffic • lls - Enable Link-local Signaling (LLS) mode • none - hitless restart (graceful restart) is disabled	`none`
`restart-period <time_int>`	Enter the time in seconds the restart is expected to take.	`120`
`rfc1583-compatible {enable | disable}`	Enable or disable RFC 1583 compatibility. RFC 1583 compatibility should be enabled only when there is another OSPF router in the network that only supports RFC 1583. When RFC 1583 compatibility is enabled, routers choose the path with the lowest cost. Otherwise, routers choose the lowest cost intra-area path through a non-backbone area.	`disable`
`router-id <address_ipv4>`	Set the router ID. The router ID is a unique number, in IP address dotted decimal format, that is used to identify an OSPF router to other OSPF routers within an area. The router ID should not be changed while OSPF is running. A router ID of 0.0.0.0 is not allowed.	`0.0.0.0`
`spf-timers <delay_integer> <hold_integer>`	Change the default shortest path first (SPF) calculation delay time and frequency. The `delay_integer` is the time, in seconds, between when OSPF receives information that will require an SPF calculation and when it starts an SPF calculation. The valid range for `delay_integer` is 0 to 4294967295. The `hold_integer` is the minimum time, in seconds, between consecutive SPF calculations. The valid range for `hold_integer` is 0 to 4294967295. OSPF updates routes more quickly if the SPF timers are set low; however, this uses more CPU. A setting of 0 for `spf-timers` can quickly use up all available CPU.	`5 10`

Example

This example shows how to set the OSPF router ID to 1.1.1.1 for a standard area border router:

```
config router ospf
  set abr-type standard
  set router-id 1.1.1.1
end
```

config area

Use this subcommand to set OSPF area related parameters. Routers in an OSPF autonomous system (AS) or routing domain are organized into logical groupings called areas. Areas are linked together by area border routers (ABRs). There must be a backbone area that all areas can connect to. You can use a virtual link to connect areas that do not have a physical connection to the backbone. Routers within an OSPF area maintain link state databases for their own areas.

FortiGate units support the three main types of areas—stub areas, Not So Stubby areas (NSSA), and regular areas. A stub area only has a default route to the rest of the OSPF routing domain. NSSA is a type of stub area that can import AS external routes and send them to the backbone, but cannot receive AS external routes from the backbone or other areas. All other areas are considered regular areas.

You can use the `config filter-list` subcommand to control the import and export of LSAs into and out of an area. For more information, see “config filter-list variables” on page 320.

You can use access or prefix lists for OSPF area filter lists. For more information, see “access-list, access-list6” on page 276 and “prefix-list, prefix-list6” on page 337.

You can use the `config range` subcommand to summarize routes at an area boundary. If the network numbers in an area are contiguous, the ABR advertises a summary route that includes all the networks within the area that are within the specified range. See “config range variables” on page 320.

You can configure a virtual link using the `config virtual-link` subcommand to connect an area to the backbone when the area has no direct connection to the backbone (see “config virtual-link variables” on page 320). A virtual link allows traffic from the area to transit a directly connected area to reach the backbone. The transit area cannot be a stub area. Virtual links can only be set up between two ABRs.

Note: If you define a filter list, the `direction` and `list` fields are required. If you define a range, the `prefix` field is required. If you define a virtual link, the `peer` field is required. All other fields are optional.

Note: If you configure authentication for interfaces, the authentication configured for the area is overridden.

Variable	Description	Default
`edit <area_address_ipv4>`	Type the IP address of the area. An address of 0.0.0.0 indicates the backbone area.	No default.
`authentication {md5 | none | text}`	Define the authentication used for OSPF packets sent and received in this area. Choose one of: **`none`** — no authentication is used. **`text`** — the authentication key is sent as plain text. **`md5`** — the authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the OSPF packet, not the confidentiality of the information in the packet. In text mode the key is sent in clear text over the network, and is only used to prevent network problems that can occur if a misconfigured router is mistakenly added to the area. Authentication passwords or keys are defined per interface. For more information, see “config ospf-interface” on page 324.	`none`
`default-cost <cost_integer>`	Enter the metric to use for the summary default route in a stub area or not so stubby area (NSSA). A lower default cost indicates a more preferred route. The valid range for `cost_integer` is 1 to 16777214.	`10`
`nssa-default-information-originate {enable | disable}`	Enter `enable` to advertise a default route in a not so stubby area. Affects NSSA ABRs or NSSA Autonomous System Boundary Routers only.	`disable`
`nssa-default-information-originate-metric <metric>`	Specify the metric (an integer) for the default route set by the `nssa-default-information-originate` field.	`10`
`nssa-default-information-originate-metric-type {1 | 2}`	Specify the OSPF external metric type for the default route set by the `nssa-default-information-originate` field.	`2`
`nssa-redistribution {enable | disable}`	Enable or disable redistributing routes into a NSSA area.	`enable`

Variable	Description	Default
nssa-translator-role {always | candidate | never}	A NSSA border router can translate the Type 7 LSAs used for external route information within the NSSA to Type 5 LSAs used for distributing external route information to other parts of the OSPF routing domain. Usually a NSSA will have only one NSSA border router acting as a translator for the NSSA. You can set the translator role to always to ensure this FortiGate unit always acts as a translator if it is in a NSSA, even if other routers in the NSSA are also acting as translators. You can set the translator role to candidate to have this FortiGate unit participate in the process for electing a translator for a NSSA. You can set the translator role to never to ensure this FortiGate unit never acts as the translator if it is in a NSSA.	candidate
shortcut {default | disable | enable}	Use this command to specify area shortcut parameters.	disable
stub-type {no-summary | summary}	Enter no-summary to prevent an ABR sending summary LSAs into a stub area. Enter summary to allow an ABR to send summary LSAs into a stub area.	summary
type {nssa | regular | stub}	Set the area type: • Select nssa for a not so stubby area. • Select regular for a normal OSPF area. • Select stub for a stub area. For more information, see “config area” on page 318.	regular
config filter-list variables		
edit <filter-list_id>	Enter an ID number for the filter list. The number must be an integer.	No default.
direction {in | out}	Set the direction for the filter. Enter in to filter incoming packets. Enter out to filter outgoing packets.	out
list <name_str>	Enter the name of the access list or prefix list to use for this filter list.	Null.
config range variables		
edit <range_id>	Enter an ID number for the range. The number must be an integer in the 0 to 4 294 967 295 range.	No default.
advertise {enable | disable}	Enable or disable advertising the specified range.	enable
prefix <address_ipv4mask>	Specify the range of addresses to summarize.	0.0.0.0 0.0.0.0
substitute <address_ipv4mask>	Enter a prefix to advertise instead of the prefix defined for the range. The prefix 0.0.0.0 0.0.0.0 is not allowed.	0.0.0.0 0.0.0.0
substitute-status {enable | disable}	Enable or disable using a substitute prefix.	disable
config virtual-link variables		
edit <vlink_name>	Enter a name for the virtual link.	No default.
authentication {md5 | none | text}	Define the type of authentication used for OSPF packets sent and received over this virtual link. Choose one of: **none** — no authentication is used. **text** — the authentication key is sent as plain text. **md5** — the authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the OSPF packet, not the confidentiality of the information in the packet. In text mode the key is sent in clear text over the network, and is only used only to prevent network problems that can occur if a misconfigured router is mistakenly added to the area.	none

Variable	Description	Default
authentication-key <password_str>	Enter the password to use for text authentication. The maximum length for the authentication-key is 15 characters. The authentication-key used must be the same on both ends of the virtual link. This field is only available when authentication is set to text.	* (No default.)
dead-interval <seconds_integer>	The time in seconds to wait for a hello packet before declaring a router down. The value of the dead-interval should be four times the value of the hello-interval. Both ends of the virtual link must use the same value for dead-interval. The valid range for seconds_integer is 1 to 65535.	40
hello-interval <seconds_integer>	The time, in seconds, between hello packets. Both ends of the virtual link must use the same value for hello-interval. The value for dead-interval should be four times larger than the hello-interval value. The valid range for seconds_integer is 1 to 65535.	10
md5-key <id_integer><key_str>	This field is available when authentication is set to md5. Enter the key ID and password to use for MD5 authentication. Both ends of the virtual link must use the same key ID and key. The valid range for id_integer is 1 to 255. key_str is an alphanumeric string of up to 16 characters.	No default.
peer <address_ipv4>	The router id of the remote ABR. 0.0.0.0 is not allowed.	0.0.0.0
retransmit-interval <seconds_integer>	The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for seconds_integer is 1 to 65535.	5
transmit-delay <seconds_integer>	The estimated time, in seconds, required to send a link state update packet on this virtual link. OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the virtual link. Increase the value for transmit-delay on low speed links. The valid range for seconds_integer is 1 to 65535.	1

Example

This example shows how to configure a stub area with the id 15.1.1.1, a stub type of summary, a default cost of 20, and MD5 authentication.

```
config router ospf
  config area
    edit 15.1.1.1
      set type stub
      set stub-type summary
      set default-cost 20
      set authentication md5
    end
  end
```

This example shows how to use a filter list named acc_list1 to filter packets entering area 15.1.1.1.

```
config router ospf
  config area
    edit 15.1.1.1
      config filter-list
```

```
      edit 1
        set direction in
        set list acc_list1
      end
  end
```

This example shows how to set the prefix for range 1 of area 15.1.1.1.

```
config router ospf
  config area
    edit 15.1.1.1
      config range
        edit 1
          set prefix 1.1.0.0 255.255.0.0
        end
    end
```

This example shows how to configure a virtual link.

```
config router ospf
  config area
    edit 15.1.1.1
      config virtual-link
        edit vlnk1
          set peer 1.1.1.1
        end
    end
```

config distribute-list

Use this subcommand to filter the networks for routing updates using an access list. Routes not matched by any of the distribution lists will not be advertised.

You must configure the access list that you want the distribution list to use before you configure the distribution list. To configure an access list, see “access-list, access-list6” on page 276.

Note: The `access-list` and `protocol` fields are required.

Variable	Description	Default
`edit <distribute-list_id>`	Enter an ID number for the distribution list. The number must be an integer.	No default.
`access-list <name_str>`	Enter the name of the access list to use for this distribution list.	`Null.`
`protocol {connected | rip | static}`	Advertise only the routes discovered by the specified protocol and that are permitted by the named access list.	`connected`

Example

This example shows how to configure distribution list 2 to use an access list named `acc_list1` for all static routes.

```
config router ospf
  config distribute-list
    edit 2
      set access-list acc_list1
      set protocol static
    end
```

```
end
```

config neighbor

Use this subcommand to manually configure an OSPF neighbor on non-broadcast networks. OSPF packets are unicast to the specified neighbor address. You can configure multiple neighbors.

Note: The `ip` field is required. All other fields are optional.

Variable	Description	Default
`edit <neighbor_id>`	Enter an ID number for the OSPF neighbor. The number must be an integer.	No default.
`cost <cost_integer>`	Enter the cost to use for this neighbor. The valid range for `cost_integer` is 1 to 65535.	`10`
`ip <address_ipv4>`	Enter the IP address of the neighbor.	`0.0.0.0`
`poll-interval <seconds_integer>`	Enter the time, in seconds, between hello packets sent to the neighbor in the down state. The value of the poll interval must be larger than the value of the hello interval. The valid range for `seconds_integer` is 1 to 65535.	`10`
`priority <priority_integer>`	Enter a priority number for the neighbor. The valid range for `priority_integer` is 0 to 255.	`1`

Example

This example shows how to manually add a neighbor.

```
config router ospf
  config neighbor
    edit 1
      set ip 192.168.21.63
    end
  end
```

config network

Use this subcommand to identify the interfaces to include in the specified OSPF area. The `prefix` field can define one or multiple interfaces.

Note: The `area` and `prefix` fields are required.

Variable	Description	Default
`edit <network_id>`	Enter an ID number for the network. The number must be an integer.	No default.
`area <id-address_ipv4>`	The ID number of the area to be associated with the prefix.	`0.0.0.0`
`prefix <address_ipv4mask>`	Enter the IP address and netmask for the OSPF network.	`0.0.0.0 0.0.0.0`

Example

Use the following command to enable OSPF for the interfaces attached to networks specified by the IP address 10.0.0.0 and the netmask 255.255.255.0 and to add these interfaces to area 10.1.1.1.

```
config router ospf
  config network
```

```
    edit 2
      set area 10.1.1.1
      set prefix 10.0.0.0 255.255.255.0
    end
  end
```

config ospf-interface

Use this subcommand to configure interface related OSPF settings.

Note: The `interface` field is required. All other fields are optional.

Note: If you configure authentication for the interface, authentication for areas is not used.

Variable	Description	Default
`edit <ospf_interface_name>`	Enter a descriptive name for this OSPF interface configuration. To apply this configuration to a FortiGate unit interface, set the `interface <name_str>` attribute.	No default.
`authentication {md5 | none | text}`	Define the authentication used for OSPF packets sent and received by this interface. Choose one of: **none** — no authentication is used. **text** — the authentication key is sent as plain text. **md5** — the authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the update packet, not the confidentiality of the routing information in the packet. In text mode the key is sent in clear text over the network, and is only used only to prevent network problems that can occur if a misconfigured router is mistakenly added to the network. All routers on the network must use the same authentication type.	`none`
`authentication-key <password_str>`	This field is available when `authentication` is set to `text`. Enter the password to use for `text` authentication. The `authentication-key` must be the same on all neighboring routers. The maximum length for the `authentication-key` is 15 characters.	* (No default.)
`bfd {enable | disable}`	Select to enable Bi-directional Forwarding Detection (BFD). It is used to quickly detect hardware problems on the network. This command enables this service on this interface.	
`cost <cost_integer>`	Specify the cost (metric) of the link. The cost is used for shortest path first calculations.	`10`
`database-filter-out {enable | disable}`	Enable or disable flooding LSAs out of this interface.	`disable`
`dead-interval <seconds_integer>`	The time, in seconds, to wait for a hello packet before declaring a router down. The value of the `dead-interval` should be four times the value of the `hello-interval`. All routers on the network must use the same value for `dead-interval`. The valid range for `seconds_integer` is 1 to 65535.	`40`

Variable	Description	Default
hello-interval <seconds_integer>	The time, in seconds, between hello packets. All routers on the network must use the same value for hello-interval. The value of the dead-interval should be four times the value of the hello-interval. The valid range for seconds_integer is 1 to 65535.	10
interface <name_str>	Enter the name of the interface to associate with this OSPF configuration. The interface might be a virtual IPSec or GRE interface.	Null.
ip <address_ipv4>	Enter the IP address of the interface named by the interface field. It is possible to apply different OSPF configurations for different IP addresses defined on the same interface.	0.0.0.0
md5-key <id_integer> <key_str>	This field is available when authentication is set to md5. Enter the key ID and password to use for MD5 authentication You can add more than one key ID and key pair per interface. However, you cannot unset one key without unsetting all of the keys. The key ID and key must be the same on all neighboring routers. The valid range for id_integer is 1 to 255. key_str is an alphanumeric string of up to 16 characters.	No default.
mtu <mtu_integer>	Change the Maximum Transmission Unit (MTU) size included in database description packets sent out this interface. The valid range for mtu_integer is 576 to 65535.	1500
mtu-ignore {enable | disable}	Use this command to control the way OSPF behaves when the Maximum Transmission Unit (MTU) in the sent and received database description packets does not match. When mtu-ignore is enabled, OSPF will stop detecting mismatched MTUs and go ahead and form an adjacency. When mtu-ignore is disabled, OSPF will detect mismatched MTUs and not form an adjacency. mtu-ignore should only be enabled if it is not possible to reconfigure the MTUs so that they match on both ends of the attempted adjacency connection.	disable
network-type <type>	Specify the type of network to which the interface is connected. OSPF supports four different types of network. This command specifies the behavior of the OSPF interface according to the network type. Choose one of: **broadcast** **non-broadcast** **point-to-multipoint** **point-to-point** If you specify non-broadcast, you must also configure neighbors using "config neighbor" on page 323.	broadcast
priority <priority_integer>	Set the router priority for this interface. Router priority is used during the election of a designated router (DR) and backup designated router (BDR). An interface with router priority set to 0 can not be elected DR or BDR. The interface with the highest router priority wins the election. If there is a tie for router priority, router ID is used. Point-to-point networks do not elect a DR or BDR; therefore, this setting has no effect on a point-to-point network. The valid range for priority_integer is 0 to 255.	1
resync-timeout <integer>	Enter the synchronizing timeout for graceful restart interval in seconds. This is the period for this interface to synchronize with a neighbor.	40
retransmit-interval <seconds_integer>	The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for seconds_integer is 1 to 65535.	5

Variable	Description	Default
status {enable | disable}	Enable or disable OSPF on this interface.	enable
transmit-delay <seconds_integer>	The estimated time, in seconds, required to send a link state update packet on this interface. OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the interface. Increase the value for transmit-delay on low speed links. The valid range for seconds_integer is 1 to 65535.	1

Example

This example shows how to assign an OSPF interface configuration named test to the interface named internal and how to configure text authentication for this interface.

```
config router ospf
  config ospf-interface
    edit test
      set interface internal
      set ip 192.168.20.3
      set authentication text
      set authentication-key a2b3c4d5e
    end
  end
```

config redistribute

Use this subcommand to redistribute routes learned from BGP, RIP, static routes, or a direct connection to the destination network.

The OSPF redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- bgp — Redistribute routes learned from BGP.
- connected — Redistribute routes learned from a direct connection to the destination network.
- static — Redistribute the static routes defined in the FortiGate unit routing table.
- rip — Redistribute routes learned from RIP.

When you enter the subcommand, end the command with one of the four static entry names (that is, config redistribute {bgp | connected | static | rip}).

Note: All fields are optional.

Variable	Description	Default
metric <metric_integer>	Enter the metric to be used for the redistributed routes. The metric_integer range is from 1 to 16777214.	10
metric-type {1 | 2}	Specify the external link type to be used for the redistributed routes.	2
routemap <name_str>	Enter the name of the route map to use for the redistributed routes. For information on how to configure route maps, see “route-map” on page 354.	Null.
status {enable | disable}	Enable or disable redistributing routes.	disable
tag <tag_integer>	Specify a tag for redistributed routes. The valid range for tag_integer is 0 to 4294967295.	0

Example

This example shows how to enable route redistribution from RIP, using a metric of 3 and a route map named rtmp2.

```
config router ospf
  config redistribute rip
    set metric 3
    set routemap rtmp2
    set status enable
  end
```

config summary-address

Use this subcommand to summarize external routes for redistribution into OSPF. This command works only for summarizing external routes on an Autonomous System Boundary Router (ASBR). For information on summarization between areas, see "config range variables" on page 320. By replacing the LSAs for each route with one aggregate route, you reduce the size of the OSPF link-state database.

Note: The `prefix` field is required. All other fields are optional.

Variable	Description	Default
`edit <summary-address_id>`	Enter an ID number for the summary address. The number must be an integer.	No default.
`advertise {enable | disable}`	Advertise or suppress the summary route that matches the specified prefix.	`enable`
`prefix <address_ipv4mask>`	Enter the prefix (IP address and netmask) to use for the summary route. The prefix `0.0.0.0 0.0.0.0` is not allowed.	`0.0.0.0 0.0.0.0`
`tag <tag_integer>`	Specify a tag for the summary route. The valid range for `tag_integer` is 0 to 4294967295.	`0`

Example

This example shows how to summarize routes using the prefix 10.0.0.0 255.0.0.0.

```
config router ospf
  config summary-address
    edit 5
      set prefix 10.0.0.0 255.0.0.0
    end
  end
```

History

FortiOS v2.80	New.
FortiOS v3.0	Added `distance-external`, `distance-inter-area`, `distance-intra-area`, and `distribute-list-in` fields. Changed default value of `abr-type` field to `standard`.
FortiOS v3.0 MR4	`Added bfd, restart-mode, resynch-timeout, and restart-period fields.`

Related topics

- router access-list, access-list6
- get router info ospf, get router info protocols, get router info routing-table
- router prefix-list, prefix-list6, router route-map

ospf6

Use this command to configure OSPF routing for IPv6 traffic.

IP version 6 for OSPF is supported through Open Shortest Path First version 3 (OSPFv3) defined in RFC 2740. This includes the Authentication/Confidentiality for OSPFv3.

For more information on OSPF features in general, see "config router ospf" on page 316.

Syntax

```
config router ospf6
  set abr-type {cisco | ibm | standard}
  set auto-cost-ref-bandwidth <mbps_integer>
  set default-metric <metric_integer>
  set passive-interface <name_str>
  set router-id <address_ipv4>
  set spf-timers <delay_integer> <hold_integer>
  config area
    edit <area_address_ipv4>
      set default-cost <cost_integer>
      set stub-type {no-summary | summary}
      set type {nssa | regular | stub}
    end
  config ospf-interface
      edit <ospf_interface_name>
        set authentication {md5 | none | text}
        set cost <cost_integer>
        set dead-interval <seconds_integer>
        set hello-interval <seconds_integer>
        set interface <name_str>
        set priority <priority_integer>
        set retransmit-interval <seconds_integer>
        set status {enable | disable}
        set transmit-delay <seconds_integer>
      end
    end
    config redistribute {bgp | connected | rip | static}
      set metric <metric_integer>
      set metric-type {1 | 2}
      set routemap <name_str>
      set status {enable | disable}
    end
  end
```

Variable	Description	Default
`abr-type {cisco | ibm | standard}`	Specify the behavior of a FortiGate unit acting as an OSPF area border router (ABR) when it has multiple attached areas and has no backbone connection. Selecting the ABR type compatible with the routers on your network can reduce or eliminate the need for configuring and maintaining virtual links. For more information, see RFC 3509.	`standard`
`auto-cost-ref-bandwidth <mbps_integer>`	Enter the Mbits per second for the reference bandwidth. Values can range from 1 to 65535.	1000

Variable	Description	Default
default-metric <metric_integer>	Specify the default metric that OSPF should use for redistributed routes. The valid range for metric_integer is 1 to 16777214.	10
passive-interface <name_str>	OSPF routing information is not sent or received through the specified interface.	No default.
router-id <address_ipv4>	Set the router ID. The router ID is a unique number, in IP address dotted decimal format, that is used to identify an OSPF router to other OSPF routers within an area. The router ID should not be changed while OSPF is running. A router ID of 0.0.0.0 is not allowed.	0.0.0.0
spf-timers <delay_integer> <hold_integer>	Change the default shortest path first (SPF) calculation delay time and frequency. The delay_integer is the time, in seconds, between when OSPF receives information that will require an SPF calculation and when it starts an SPF calculation. The valid range for delay_integer is 0 to 4294967295. The hold_integer is the minimum time, in seconds, between consecutive SPF calculations. The valid range for hold_integer is 0 to 4294967295. OSPF updates routes more quickly if the SPF timers are set low; however, this uses more CPU. A setting of 0 for spf-timers can quickly use up all available CPU.	5 10

config area

Use this subcommand to set OSPF area related parameters. Routers in an OSPF autonomous system (AS) or routing domain are organized into logical groupings called areas. Areas are linked together by area border routers (ABRs). There must be a backbone area that all areas can connect to. You can use a virtual link to connect areas that do not have a physical connection to the backbone. Routers within an OSPF area maintain link state databases for their own areas.

You can use the config range subcommand to summarize routes at an area boundary. If the network numbers in an area are contiguous, the ABR advertises a summary route that includes all the networks within the area that are within the specified range. See “config range variables” on page 320.

You can configure a virtual link using the config virtual-link subcommand to connect an area to the backbone when the area has no direct connection to the backbone (see “config virtual-link variables” on page 320). A virtual link allows traffic from the area to transit a directly connected area to reach the backbone. The transit area cannot be a stub area. Virtual links can only be set up between two ABRs.

Variable	Description	Default
edit <area_address_ipv4>	Type the IP address of the area. An address of 0.0.0.0 indicates the backbone area.	No default.
default-cost <cost_integer>	Enter the metric to use for the summary default route in a stub area or not so stubby area (NSSA). A lower default cost indicates a more preferred route. The valid range for cost_integer is 1 to 16777214.	10
stub-type {no-summary | summary}	Select the type of communication with the stub area. Choose one of: **no-summary** — prevent an ABR sending summary LSAs into a stub area. **summary** — allow an ABR to send summary LSAs into a stub area.	summary
type {regular | stub}	For the type of area, choose one of: **regular** — for a normal OSPF area. **stub** — for a stub area that has limited connections to other areas.	regular

Variable	Description	Default
config range Variables		
edit <range_id>	Enter an ID number for the range. The number must be an integer in the 0 to 4 294 967 295 range.	No default.
advertise {enable | disable}	Enable or disable advertising the specified range.	enable
prefix6 <address_ipv6mask>	Specify the range of addresses to summarize.	::/0
config virtual-link Variables		
edit <vlink_name>	Enter a name for the virtual link.	No default.
dead-interval <seconds_integer>	The time, in seconds, to wait for a hello packet before declaring a router down. The value of the dead-interval should be four times the value of the hello-interval. Both ends of the virtual link must use the same value for dead-interval. The valid range for seconds_integer is 1 to 65535.	40
hello-interval <seconds_integer>	The time, in seconds, between hello packets. Both ends of the virtual link must use the same value for hello-interval. The valid range for seconds_integer is 1 to 65535.	10
peer <address_ipv4>	The router id of the remote ABR. 0.0.0.0 is not allowed.	0.0.0.0
retransmit-interval <seconds_integer>	The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for seconds_integer is 1 to 65535.	5
transmit-delay <seconds_integer>	The estimated time, in seconds, required to send a link state update packet on this virtual link. OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the virtual link. Increase the value for transmit-delay on low speed links. The valid range for seconds_integer is 1 to 65535.	1

config ospf6-interface

Use this subcommand to change interface related OSPF settings.

Note: The interface field is required. All other fields are optional.

Variable	Description	Default
edit <ospf_interface_name>	Enter a descriptive name for this OSPF interface configuration. To apply this configuration to a FortiGate unit interface, set the interface <name_str> attribute.	No default.
area-id <ip4_addr>	Enter the area ID in A.B.C.D IPv4 format.	0.0.0.0
cost <cost_integer>	Specify the cost (metric) of the link. The cost is used for shortest path first calculations. Range 1 to 65 535. Use 0 for auto-cost.	0

Variable	Description	Default
dead-interval <seconds_integer>	The time, in seconds, to wait for a hello packet before declaring a router down. The value of the dead-interval should be four times the value of the hello-interval. All routers on the network must use the same value for dead-interval. The valid range for seconds_integer is 1 to 65535.	40
hello-interval <seconds_integer>	The time, in seconds, between hello packets. All routers on the network must use the same value for hello-interval. The valid range for seconds_integer is 1 to 65535.	10
interface <name_str>	Enter the name of the interface to associate with this OSPF configuration. The interface might be a virtual IPSec or GRE interface.	Null
priority <priority_integer>	Set the router priority for this interface. Router priority is used during the election of a designated router (DR) and backup designated router (BDR). An interface with router priority set to 0 can not be elected DR or BDR. The interface with the highest router priority wins the election. If there is a tie for router priority, router ID is used. Point-to-point networks do not elect a DR or BDR; therefore, this setting has no effect on a point-to-point network. The valid range for priority_integer is 0 to 255.	1
retransmit-interval <seconds_integer>	The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for seconds_integer is 1 to 65535.	5
status {enable | disable}	Enable or disable OSPF on this interface.	enable
transmit-delay <seconds_integer>	The estimated time, in seconds, required to send a link state update packet on this interface. OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the interface. Increase the value for transmit-delay on low speed links. The valid range for seconds_integer is 1 to 65535.	1

config redistribute

Use this subcommand to redistribute routes learned from BGP, RIP, static routes, or a direct connection to the destination network.

The OSPF redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- bgp — Redistribute routes learned from BGP.
- connected — Redistribute routes learned from a direct connection to the destination network.
- static — Redistribute the static routes defined in the FortiGate unit routing table.
- rip — Redistribute routes learned from RIP.

When you enter the subcommand, end the command with one of the four static entry names (that is, config redistribute {bgp | connected | rip | static}).

Note: All fields are optional.

Variable	Description	Default
`metric <metric_integer>`	Enter the metric to be used for the redistributed routes. The `metric_integer` range is from 1 to 16777214.	`10`
`metric-type {1 | 2}`	Specify the external link type to be used for the redistributed routes.	`2`
`routemap <name_str>`	Enter the name of the route map to use for the redistributed routes.	`Null.`
`status {enable | disable}`	Enable or disable redistributing routes.	`disable`

History

FortiOS v4.0 MR1 New.

policy

Use this command to add, move, edit or delete a route policy. When you create a policy route, any packets that match the policy are forwarded to the IP address of the next-hop gateway through the specified outbound interface.

You can configure the FortiGate unit to route packets based on:

- a source address
- a protocol, service type, or port range
- the inbound interface
- type of service (TOS)

When the FortiGate unit receives a packet, it starts at the top of the policy routing list and attempts to match the packet with a policy in ascending order. If no packets match the policy route, the FortiGate unit routes the packet using the routing table. Route policies are processed before static routing. You can change the order of policy routes using the `move` command.

Note: For static routing, any number of static routes can be defined for the same destination. When multiple routes for the same destination exist, the FortiGate unit chooses the route having the lowest administrative distance. Route redundancy is not available for policy routing: any packets that match a route policy are forwarded according to the route specified in the policy.

Type of service (TOS) is an 8-bit field in the IP header that enables you to determine how the IP datagram should be delivered, with such criteria as delay, priority, reliability, and minimum cost. Each quality helps gateways determine the best way to route datagrams. A router maintains a ToS value for each route in its routing table. The lowest priority TOS is 0, the highest is 7 - when bits 3, 4, and 5 are all set to 1. The router tries to match the TOS of the datagram to the TOS on one of the possible routes to the destination. If there is no match, the datagram is sent over a zero TOS route. Using increased quality may increase the cost of delivery because better performance may consume limited network resources. For more information see RFC 791 and RFC 1349.

Table 9: The role of each bit in the IP header TOS 8-bit field

bits 0, 1, 2	**Precedence**	Some networks treat high precedence traffic as more important traffic. Precedence should only be used within a network, and can be used differently in each network. Typically you do not care about these bits.
bit 3	**Delay**	When set to 1, this bit indicates low delay is a priority. This is useful for such services as VoIP where delays degrade the quality of the sound.
bit 4	**Throughput**	When set to 1, this bit indicates high throughput is a priority. This is useful for services that require lots of bandwidth such as video conferencing.
bit 5	**Reliability**	When set to 1, this bit indicates high reliability is a priority. This is useful when a service must always be available such as with DNS servers.
bit 6	**Cost**	When set to 1, this bit indicates low cost is a priority. Generally there is a higher delivery cost associated with enabling bits 3,4, or 5, and bit 6 indicates to use the lowest cost route.
bit 7	**Reserved for future use**	Not used at this time.

The two fields `tos` and `tos-mask` enable you to configure type of service support on your FortiGate unit. `tos-mask` enables you to only look at select bits of the 8-bit TOS field in the IP header. This is useful as you may only care about reliability for some traffic, and not about the other TOS criteria.

The value in `tos` is used to match the pattern from `tos-mask`. If it matches, then the rest of the policy is applied. If the mask doesn't match, the next policy tries to match if its configured, and eventually default routing is applied if there are no other matches.

Note: You need to use `tos-mask` to remove bits from the pattern you don't care about, or those bits will prevent a match with your `tos` pattern.

Syntax

```
config router policy
  move <seq-num1> {before | after} <seq-num2>
  edit <policy_integer>
    set dst <dest-address_ipv4mask>
    set end-port <port_integer>
    set gateway <address_ipv4>
    set input-device <interface-name_str>
    set output-device <interface-name_str>
    set protocol <protocol_integer>
    set src <source-address_ipv4mask>
    set start-port <port_integer>
    set tos <hex_mask>
    set tos-mask <hex_mask>
  end
```

Note: The `input-device` field is required. All other fields are optional.

Variable	Description	Default
`move <seq-num1> {before | after} <seq-num2>`	Move policy <seq-num1> to before or after policy. <seq-num2>.	No default.
`edit <policy_integer>`	Enter an ID number for the route policy. The number must be an integer.	No default.
`dst <dest-address_ipv4mask>`	Match packets that have this destination IP address and netmask.	`0.0.0.0 0.0.0.0`
`end-port <port_integer>`	The end port number of a port range for a policy route. Match packets that have this destination port range. You must configure both the `start-port` and `end-port` fields for destination-port-range matching to take effect. To specify a range, the `start-port` value must be lower than the `end-port` value. To specify a single port, the `start-port` value must be identical to the `end-port` value. The `port_integer` range is 0 to 65 535. For protocols other than 7 (TCP) and 17 (UDP), the port number is ignored.	`65 535`
`gateway <address_ipv4>`	Send packets that match the policy to this next hop router.	`0.0.0.0`
`input-device <interface-name_str>`	Match packets that are received on this interface.	`Null.`
`output-device <interface-name_str>`	Send packets that match the policy out this interface.	`Null.`

Variable	Description	Default
protocol <protocol_integer>	To perform policy routing based on the value in the protocol field of the packet, enter the protocol number to match. The Internet Protocol Number is found in the IP packet header. RFC 5237 describes protocol numbers and you can find a list of the assigned protocol numbers here. The range is from 0 to 255. A value of 0 disables the feature. **Tip:** Commonly used *protocol* settings include 6 to route TCP sessions, 17 for UDP sessions, 1 for ICMP sessions, 47 for GRE sessions, and 92 for multicast sessions. For protocols other than 6 and UDP, the port number is ignored.	0
src <source-address_ipv4mask>	Match packets that have this source IP address and netmask.	0.0.0.0 0.0.0.0
start-port <port_integer>	The start port number of a port range for a policy route. Match packets that have this destination port range. You must configure both the start-port and end-port fields for destination-port-range matching to take effect. To specify a range, the start-port value must be lower than the end-port value. To specify a single port, the start-port value must be identical to the end-port value. The port_integer range is 0 to 65 535. For protocols other than 7 (TCP) and 17 (UDP), the port number is ignored.	1
tos <hex_mask>	The type of service (TOS) mask to match after applying the tos-mask. This is an 8-bit hexadecimal pattern that can be from "00" to "FF". The tos mask attempts to match the quality of service for this profile. Each bit in the mask represents a different aspect of quality. A tos mask of "0010" would indicate reliability is important, but with normal delay and throughput. The hex mask for this pattern would be "04".	Null.
tos-mask <hex_mask>	This value determines which bits in the IP header's TOS field are significant. This is an 8-bit hexadecimal mask that can be from "00" to "FF". Typically, only bits 3 through 6 are used for TOS, so it is necessary to mask out the other bits. To mask out everything but bits 3 through 6, the hex mask would be "1E".	Null.

Example

If a FortiGate unit provides Internet access for multiple internal subnets, you can use policy routing to control the route that traffic from each network takes to the Internet. For example, if the internal network includes the subnets 192.168.10.0 and 192.168.20.0 you can enter the following route policies:

- Enter the following command to route traffic from the 192.168.10.0 subnet to the 100.100.100.0 subnet. Force the packets to the next hop gateway at IP address 1.1.1.1 through the interface named external.

```
config router policy
  edit 1
    set input-device internal
    set src 192.168.10.0 255.255.255.0
    set dst 100.100.100.0 255.255.255.0
    set output-device external
    set gateway 1.1.1.1
  end
```

- Enter the following command to route traffic from the 192.168.20.0 subnet to the 200.200.200.0 subnet. Force the packets to the next hop gateway at IP address 2.2.2.1 through the interface named external.

```
config router policy
  edit 2
    set input-device internal
    set src 192.168.20.0 255.255.255.0
    set dst 200.200.200.0 255.255.255.0
    set output-device external
    set gateway 2.2.2.1
  end
```

- Enter the following command to direct all HTTP traffic using port 80 to the next hop gateway at IP address 1.1.1.1 if it has the TOS low delay bit set.

```
config router policy
  edit 1
    set input-device internal
    set src 0.0.0.0 0.0.0.0
    set dst 0.0.0.0 0.0.0.0
    set output-device external
    set gateway 1.1.1.1
    set protocol 6
    set start-port 80
    set end-port 80
    set tos-mask 10
    set tos 10
  end
```

- Enter the following command to direct all other traffic to the next hop gateway at IP address 2.2.2.1.

```
config router policy
  edit 2
    set input-device internal
    set src 0.0.0.0 0.0.0.0
    set dst 0.0.0.0 0.0.0.0
    set output-device external
    set gateway 2.2.2.1
  end
```

History

FortiOS v2.80	Revised.
FortiOS v3.0	Replaced all underscore characters in fields with hyphens. Changed default `start-point` number to 1. Changed default `end-point` number to 65 535.
FortiOS v3.0 MR7	Added `tos`, and `tos-mask`.

Related topics

- router static

prefix-list, prefix-list6

Use this command to add, edit, or delete prefix lists. A prefix list is an enhanced version of an access list that allows you to control the length of the prefix netmask. Prefix lists are called by routing protocols such as RIP or OSPF.

Each rule in a prefix list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and maximum and minimum prefix length settings.

The FortiGate unit attempts to match a packet against the rules in a prefix list starting at the top of the list. If it finds a match for the prefix it takes the action specified for that prefix. If no match is found the default action is deny. A prefix-list should be used to match the default route 0.0.0.0/0.

`config router setting` uses prefix-list to filter the displayed routes. For more information, see "setting" on page 360.

Syntax

```
config router prefix-list, prefix-list6
  edit <prefix_list_name>
    set comments <string>
    config rule
      edit <prefix_rule_id>
        set action {deny | permit}
        set ge <length_integer>
        set le <length_integer>
        set prefix {<address_ipv4mask> | any}
        set prefix6 {<address_ipv6mask> | any}
      end
  end
```

Note: The `action` and `prefix` fields are required. All other fields are optional.

Variable	Description	Default
`edit <prefix_list_name>`	Enter a name for the prefix list. A prefix list and an access list cannot have the same name.	No default.
config rule variables		
`edit <prefix_rule_id>`	Enter an entry number for the rule. The number must be an integer.	No default.
`action {deny | permit}`	Set the action to take for this prefix.	`permit`
`comments <string>`	Enter a description of this access list entry. The description can be up to 127 characters long.	
`ge <length_integer>`	Match prefix lengths that are greater than or equal to this number. The setting for `ge` should be less than the setting for `le`. The setting for `ge` should be greater than the netmask set for `prefix`. `length_integer` can be any number from 0 to 32.	`0`
`le <length_integer>`	Match prefix lengths that are less than or equal to this number. The setting for `le` should be greater than the setting for `ge`. `length_integer` can be any number from 0 to 32.	`32`

Variable	Description	Default
prefix {<address_ipv4mask> | any}	Enter the prefix (IPv4 address and netmask) for this prefix list rule or enter any to match any prefix. The length of the netmask should be less than the setting for ge. If prefix is set to any, ge and le should not be set. This variable only available for prefix-list command.	0.0.0.0 0.0.0.0
prefix6 {<address_ipv6mask> | any}	Enter the prefix (IPv6 address and netmask) for this prefix list rule or enter any to match any prefix. The length of the netmask should be less than the setting for ge. If prefix6 is set to any, ge and le should not be set. This variable only available for prefix-list6 command.	::/0

Examples

This example shows how to add a prefix list named prf_list1 with three rules. The first rule permits subnets that match prefix lengths between 26 and 30 for the prefix 192.168.100.0 255.255.255.0. The second rule denies subnets that match the prefix lengths between 20 and 25 for the prefix 10.1.0.0 255.255.0.0. The third rule denies all other traffic.

```
config router prefix-list
  edit prf_list1
    config rule
      edit 1
        set prefix 192.168.100.0 255.255.255.0
        set action permit
        set ge 26
        set le 30
      next
      edit 2
        set prefix 10.1.0.0 255.255.0.0
        set action deny
        set ge 20
        set le 25
      next
      edit 3
        set prefix any
        set action deny
      end
  end
```

The following example shows how to create a prefix-list that will drop the default route but allow all other prefixes to be passed. The first rule matches the default route only and is set to deny, the second rule will match all other prefixes and allow them to be passed.

```
config router prefix-list
  edit "drop_default"
    config rule
    edit 1
      set action deny
      set prefix 0.0.0.0 0.0.0.0
      unset ge
      unset le
    next
    edit 2
      set prefix any
      unset ge
```

```
      unset le
    next
    end
    next
  end
```

History

FortiOS v2.80 New.

FortiOS v2.80 MR2 Changed default for `le` from 0 to 32.

FortiOS v4.0 MR1 Added `prefix-list6` command.

Related topics

- router access-list, access-list6
- router ospf
- router ospf6
- router rip
- router ripng
- router setting

rip

Use this command to configure the Routing Information Protocol (RIP) on the FortiGate unit. RIP is a distance-vector routing protocol intended for small, relatively homogeneous networks. RIP uses hop count as its routing metric. Each network is usually counted as one hop. The network diameter is limited to 15 hops with 16 hops.

The FortiOS implementation of RIP supports RIP version 1 (see RFC 1058) and RIP version 2 (see RFC 2453). RIP version 2 enables RIP messages to carry more information, and to support simple authentication and subnet masks.

Note: `update_timer` cannot be larger than `timeout_timer` and `garbage_timer`. Attempts to do so will generate an error.

Syntax

```
config router rip
  set default-information-originate {enable | disable}
  set default-metric <metric_integer>
  set garbage-timer <timer_integer>
  set passive-interface <name_str>
  set timeout-timer <timer_integer>
  set update-timer <timer_integer>
  set version {1 2}
  config distance
    edit <distance_id>
      set access-list <name_str>
      set distance <distance_integer>
      set prefix <address_ipv4mask>
    end
  config distribute-list
    edit <distribute_list_id>
      set direction {in | out}
      set interface <name_str>
      set listname <access/prefix-listname_str>
      set status {enable | disable}
    end
  config interface
    edit <interface_name>
      set auth-keychain <name_str>
      set auth-mode {none | text | md5}
      set auth-string <password_str>
      set receive-version {1 2}
      set send-version {1 2}
      set send-version2-broadcast {enable | disable}
      set split-horizon {poisoned | regular}
      set split-horizon-status {enable | disable}
    end
  config neighbor
    edit <neighbor_id>
      set ip <address_ipv4>
    end
  config network
    edit <network_id>
```

```
    set prefix <address_ipv4mask>
  end
config offset-list
  edit <offset_list_id>
    set access-list <name_str>
    set direction {in | out}
    set interface <name_str>
    set offset <metric_integer>
    set status {enable | disable}
  end
config redistribute {connected | static | ospf | bgp}
  set metric <metric_integer>
  set routemap <name_str>
  set status {enable | disable}
end
```

config router rip

Use this command to specify RIP operating parameters.

Note: All fields are optional.

Variable	Description	Default
`default-information-originate {enable | disable}`	Enter `enable` to advertise a default static route into RIP.	`disable`
`default-metric <metric_integer>`	For non-default routes in the static routing table and directly connected networks the default metric is the metric that the FortiGate unit advertises to adjacent routers. This metric is added to the metrics of learned routes. The default metric can be a number from 1 to 16.	`1`
`garbage-timer <timer_integer>`	The time in seconds that must elapse after the timeout interval for a route expires, before RIP deletes the route. If RIP receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings. The update timer interval can not be larger than the garbage timer interval.	`120`
`passive-interface <name_str>`	Block RIP broadcasts on the specified interface. You can use "config neighbor" on page 345 and the passive interface command to allow RIP to send unicast updates to the specified neighbor while blocking broadcast updates on the specified interface.	No default.

Variable	Description	Default
`timeout-timer <timer_integer>`	The time interval in seconds after which a route is declared unreachable. The route is removed from the routing table. RIP holds the route until the garbage timer expires and then deletes the route. If RIP receives an update for the route before the timeout timer expires, then the timeout-timer is restarted. If RIP receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. The value of the timeout timer should be at least three times the value of the update timer. RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings. The update timer interval can not be larger than the timeout timer interval.	`180`
`update-timer <timer_integer>`	The time interval in seconds between RIP updates. RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings. The update timer interval can not be larger than timeout or garbage timer intervals.	`30`
`version {1 2}`	Enable sending and receiving RIP version 1 packets, RIP version 2 packets, or both for all RIP-enabled interfaces. You can override this setting on a per interface basis using the receive-version {1 2}and send-version {1 2} fields described under “config interface” on page 344.	`2`

Example

This example shows how to enable the advertising of a default static route into RIP, enable the sending and receiving of RIP version 1 packets, and raise the preference of local routes in the static routing table (the default metric) from the default of 1 to 5 - those routes well be less preferred.

```
config router rip
  set default-information-originate enable
  set version 1
  set default-metric 5
end
```

config distance

Use this subcommand to specify an administrative distance. When different routing protocols provide multiple routes to the same destination, the administrative distance sets the priority of those routes. The lowest administrative distance indicates the preferred route.

If you specify a prefix, RIP uses the specified distance when the source IP address of a packet matches the prefix.

Note: The `distance` field is required. All other fields are optional.

Variable	Description	Default
`edit <distance_id>`	Enter an ID number for the distance. The number must be an integer.	No default.
`access-list <name_str>`	Enter the name of an access list. The distances associated with the routes in the access list will be modified. To create an access list, see “access-list, access-list6” on page 276.	`Null.`

Variable	Description	Default
distance <distance_integer>	Enter a number from 1 to 255, to set the administrative distance. This field is required.	0
prefix <address_ipv4mask>	Optionally enter a prefix to apply the administrative distance to.	0.0.0.0 0.0.0.0

Example

This example shows how to change the administrative distance to 10 for all IP addresses that match the internal_example access-list.

```
config router rip
  config distance
    edit 1
      set distance 10
      set access-list internal_example
    end
  end
```

config distribute-list

Use this subcommand to filter incoming or outgoing updates using an access list or a prefix list. If you do not specify an interface, the filter will be applied to all interfaces. You must configure the access list or prefix list that you want the distribution list to use before you configure the distribution list. For more information on configuring access lists and prefix lists, see “access-list, access-list6” on page 276 and “prefix-list, prefix-list6” on page 337.

Note: The direction and listname fields are required. All other fields are optional.

Variable	Description	Default
edit <distribute_list_id>	Enter an ID number for the distribution list. The number must be an integer.	No default.
direction {in | out}	Set the direction for the filter. Enter in to filter incoming packets that originate from other routers. Enter out to filter outgoing packets the FortiGate unit is sending to other routers.	out
interface <name_str>	Enter the name of the interface to apply this distribution list to. If you do not specify an interface, this distribution list will be used for all interfaces.	Null.
listname <access/prefix-listname_str>	Enter the name of the access list or prefix list to use for this distribution list. The prefix or access list used must be configured before configuring the distribute-list.	Null.
status {enable | disable}	Enable or disable this distribution list.	disable

Example

This example shows how to configure and enable a distribution list to use an access list named allowed_routers for incoming updates on the external interface.

```
config router rip
  config distribute-list
    edit 1
      set direction in
```

```
    set interface external
    set listname allowed_routers
    set status enable
  end
end
```

config interface

Use this subcommand to configure RIP version 2 authentication, RIP version send and receive for the specified interface, and to configure and enable split horizon.

Authentication is only available for RIP version 2 packets sent and received by an interface. You must set `auth-mode` to `none` when `receive-version` or `send-version` are set to `1` or `1 2` (both are set to `1` by default).

A split horizon occurs when a router advertises a route it learns over the same interface it learned it on. In this case the router that gave the learned route to the last router now has two entries to get to another location. However, if the primary route fails that router tries the second route to find itself as part of the route and an infinite loop is created. A poisoned split horizon will still advertise the route on the interface it received it on, but it will mark the route as unreachable. Any unreachable routes are automatically removed from the routing table. This is also called split horizon with poison reverse.

Note: All fields are optional.

Variable	Description	Default
`edit <interface_name>`	Type the name of the FortiGate unit interface that is linked to the RIP network. The interface might be a virtual IPSec or GRE interface.	No default.
`auth-keychain <name_str>`	Enter the name of the key chain to use for authentication for RIP version 2 packets sent and received by this interface. Use key chains when you want to configure multiple keys. For information on how to configure key chains, see “key-chain” on page 302.	`Null.`
`auth-mode {none | text | md5}`	Use the `auth-mode` field to define the authentication used for RIP version 2 packets sent and received by this interface. Choose one of: **`none`** — no authentication is used. **`text`** — the authentication key is sent as plain text. **`md5`** — the authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the update packet, not the confidentiality of the routing information in the packet. In text mode the key is sent in clear text over the network. Text mode is usually used only to prevent network problems that can occur if an unwanted or misconfigured router is mistakenly added to the network. Use the `auth-string` field to specify the key.	`none`
`auth-string <password_str>`	Enter a single key to use for authentication for RIP version 2 packets sent and received by this interface. Use `auth-string` when you only want to configure one key. The key can be up to 35 characters long.	`Null.`
`receive-version {1 2}`	RIP routing messages are UDP packets that use port 520. Choose one of: **`1`** — configure RIP to listen for RIP version 1 messages on an interface. **`2`** — configure RIP to listen for RIP version 2 messages on an interface. **`1 2`** — configure RIP to listen for both RIP version 1 and RIP version 2 messages on an interface.	No default.

Variable	Description	Default
`send-version {1 2}`	RIP routing messages are UDP packets that use port 520. Choose one of: **1** — configure RIP to send for RIP version 1 messages on an interface. **2** — configure RIP to send for RIP version 2 messages on an interface. **1 2** — configure RIP to send for both RIP version 1 and RIP version 2 messages on an interface.	No default.
`send-version2-broadcast {enable | disable}`	Enable or disable sending broadcast updates from an interface configured for RIP version 2. RIP version 2 normally multicasts updates. RIP version 1 can only receive broadcast updates.	`disable`
`split-horizon {poisoned | regular}`	Configure RIP to use either regular or poisoned split horizon on this interface. Choose one of: **regular** — prevent RIP from sending updates for a route back out on the interface from which it received that route. **poisoned** — send updates with routes learned on an interface back out the same interface but mark those routes as unreachable.	`poisoned`
`split-horizon-status {enable | disable}`	Enable or disable split horizon for this interface. Split horizon is enabled by default. Disable split horizon only if there is no possibility of creating a counting to infinity loop when network topology changes.	`enable`

Example

This example shows how to configure the external interface to send and receive RIP version 2, to use MD5 authentication, and to use a key chain called `test1`.

```
config router rip
  config interface
    edit external
      set receive-version 2
      set send-version 2
      set auth-mode md5
      set auth-keychain test1
    end
  end
```

config neighbor

Use this subcommand to enable RIP to send unicast routing updates to the router at the specified address. You can use the `neighbor` subcommand and "passive-interface <name_str>" on page 341 to allow RIP to send unicast updates to the specified neighbor while blocking broadcast updates on the specified interface. You can configure multiple neighbors.

Note: The `ip` field is required. All other fields are optional.

Variable	Description	Default
`edit <neighbor_id>`	Enter an ID number for the RIP neighbor. The number must be an integer.	No default.
`ip <address_ipv4>`	Enter the IPv4 address of the neighboring router to which to send unicast updates.	`0.0.0.0`

Example

This example shows how to specify that the router at 192.168.21.20 is a neighbor.

```
config router rip
  config neighbor
    edit 1
      set ip 192.168.21.20
    end
  end
```

config network

Use this subcommand to identify the networks for which to send and receive RIP updates. If a network is not specified, interfaces in that network will not be advertised in RIP updates.

Note: The `prefix` field is optional.

Variable	Description	Default
`edit <network_id>`	Enter an entry number for the RIP network. The number must be an integer.	No default.
`prefix <address_ipv4mask>`	Enter the IPv4 address and netmask for the RIP network.	`0.0.0.0 0.0.0.0`

Example

Use the following command to enable RIP for the interfaces attached to networks specified by the IP address 10.0.0.0 and the netmask 255.255.255.0.

```
config router rip
  config network
    edit 2
      set prefix 10.0.0.0 255.255.255.0
    end
  end
```

config offset-list

Use this subcommand to add the specified offset to the metric (hop count) of a route from the offset list.

Note: The `access-list`, `direction`, and `offset` fields are required. All other fields are optional.

Variable	Description	Default
`edit <offset_list_id>`	Enter an ID number for the offset list. The number must be an integer.	No default.
`access-list <name_str>`	Enter the name of the access list to use for this offset list. The access list is used to determine which routes to add the metric to. For more information, see “access-list, access-list6” on page 276.	`Null.`
`direction {in | out}`	Enter `in` to apply the specified offset to the metrics of routes originating on other routers—incoming routes. Enter `out` to apply the specified offset to the metrics of routes leaving from the FortiGate unit—outgoing routes.	`out`
`interface <name_str>`	Enter the name of the interface to match for this offset list.	`Null.`

Variable	Description	Default
offset <metric_integer>	Enter the offset number to add to the metric. The metric is the hop count. The metric_integer range is from 1 to 16, with 16 being unreachable. For example if a route has already has a metric of 5, an offset of 10 will increase the metric to 15 for that route.	0
status {enable | disable}	Enable or disable this offset list.	disable

Example

This example shows how to configure and enable offset list ID number 5. This offset list entry adds a metric of 3 to incoming routes that match the access list named acc_list1 on the external interface.

```
config router rip
  config offset-list
    edit 5
      set access-list acc_list1
      set direction in
      set interface external
      set offset 3
      set status enable
    end
  end
```

config redistribute

Use this subcommand to advertise routes learned from OSPF, BGP, static routes, or a direct connection to the destination network.

The RIP redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- bgp — Redistribute routes learned from BGP.
- connected — Redistribute routes learned from a direct connection to the destination network.
- ospf — Redistribute routes learned from OSPF.
- static — Redistribute the static routes defined in the FortiGate unit routing table.

When you enter the subcommand, end the command with one of the four static entry names (that is, config redistribute {bgp | connected | ospf | static}).

Note: All fields are optional.

Variable	Description	Default
metric <metric_integer>	Enter the metric value to be used for the redistributed routes. The metric_integer range is from 0 to 16.	0
routemap <name_str>	Enter the name of the route map to use for the redistributed routes. For information on how to configure route maps, see “route-map” on page 354.	Null.
status {enable | disable}	Enable or disable advertising non-RIP routes.	disable

Example

This example shows how to enable route redistribution from OSPF, using a metric of 3 and a route map named rtmp2.

```
config router rip
```

```
config redistribute ospf
  set metric 3
  set routemap rtmp2
  set status enable
end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v2.80 MR7	Added `access-list` field to `config distance` subcommand.
FortiOS v4.0 MR1	Changed `send-version1-compatible` to `send-version2-broadcast` for `config interface`.

Related topics

- router access-list, access-list6
- router key-chain
- router prefix-list, prefix-list6
- router route-map
- get router info protocols
- get router info rip
- get router info routing-table

ripng

Use this command to configure the “next generation” Routing Information Protocol (RIPng) on the FortiGate unit. RIPng is a distance-vector routing protocol intended for small, relatively homogeneous, IPv6 networks. RIPng uses hop count as its routing metric. Each network is usually counted as one hop. The network diameter is limited to 15 hops. RIPng is defined in RFC 2080.

Syntax

```
config router ripng
  set default-information-originate {enable | disable}
  set default-metric <metric_integer>
  set garbage-timer <timer_integer>
  set passive-interface <name_str>
  set timeout-timer <timer_integer>
  set update-timer <timer_integer>
  config aggregate-address
    edit <entry-id>
      set prefix6 <aggregate_prefix>
    end
  config distribute-list
    edit <distribute_list_id>
      set direction {in | out}
      set interface <name_str>
      set listname <access/prefix-listname_str>
      set status {enable | disable}
    end
  config interface
    edit <interface_name>
      set split-horizon {poisoned | regular}
      set split-horizon-status {enable | disable}
    end
  config neighbor
    edit <neighbor_id>
      set ip <address_ipv4>
    end
  config offset-list
    edit <offset_list_id>
      set access-list <name_str>
      set direction {in | out}
      set interface <name_str>
      set offset <metric_integer>
      set status {enable | disable}
    end
  config redistribute {connected | static | ospf | bgp}
    set metric <metric_integer>
    set routemap <name_str>
    set status {enable | disable}
  end
```

Note: All fields are optional.

Variable	Description	Default
`default-information-originate {enable | disable}`	Enter `enable` to advertise a default static route into RIPng.	`disable`
`default-metric <metric_integer>`	For non-default routes in the static routing table and directly connected networks the default metric is the metric that the FortiGate unit advertises to adjacent routers. This metric is added to the metrics of learned routes. The default metric can be a number from 1 to 16.	`1`
`garbage-timer <timer_integer>`	The time in seconds that must elapse after the timeout interval for a route expires, before RIPng deletes the route. If RIPng receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings. The update timer interval can not be larger than the garbage timer interval. Range 5 to `2 147 483 647` seconds.	`120`
`passive-interface <name_str>`	Block RIPng broadcasts on the specified interface. You can use "config neighbor" on page 345 and the passive interface command to allow RIPng to send unicast updates to the specified neighbor while blocking broadcast updates on the specified interface.	No default.
`timeout-timer <timer_integer>`	The time interval in seconds after which a route is declared unreachable. The route is removed from the routing table. RIP holds the route until the garbage timer expires and then deletes the route. If RIP receives an update for the route before the timeout timer expires, then the timeout-timer is restarted. If RIP receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. The value of the timeout timer should be at least three times the value of the update timer. RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings. The update timer interval can not be larger than the timeout timer interval. Range 5 to `2 147 483 647` seconds.	`180`
`update-timer <timer_integer>`	The time interval in seconds between RIP updates. RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings. The update timer interval can not be larger than timeout or garbage timer intervals. Range 5 to `2 147 483 647` seconds.	`30`

config aggregate-address

Use this subcommand to configure aggregate address prefixes.

Variable	Description	Default
`edit <entry-id>`	Enter an entry number for the aggregate address list.	
`prefix6 <aggregate_prefix>`	Enter the prefix for the aggregate address.	`::/0`

config distribute-list

Use this subcommand to filter incoming or outgoing updates using an access list or a prefix list. If you do not specify an interface, the filter will be applied to all interfaces. You must configure the access list or prefix list that you want the distribution list to use before you configure the distribution list. For more information on configuring access lists and prefix lists, see “router access-list, access-list6” on page 276 and “router prefix-list, prefix-list6” on page 337.

Note: The `direction` and `listname` fields are required. All other fields are optional.

Variable	Description	Default
`edit <distribute_list_id>`	Enter an entry number for the distribution list. The number must be an integer.	No default.
`direction {in | out}`	Set the direction for the filter. Enter `in` to filter incoming packets. Enter `out` to filter outgoing packets.	`out`
`interface <name_str>`	Enter the name of the interface to apply this distribution list to. If you do not specify an interface, this distribution list will be used for all interfaces.	`Null.`
`listname <listname_str>`	Enter the name of the access list or prefix list to use for this distribution list.	`Null.`
`status {enable | disable}`	Enable or disable this distribution list.	`disable`

config interface

Use this subcommand to configure and enable split horizon.

A split horizon occurs when a router advertises a route it learns over the same interface it learned it on. In this case the router that gave the learned route to the last router now has two entries to get to another location. However, if the primary route fails that router tries the second route to find itself as part of the route and an infinite loop is created. A poisoned split horizon will still advertise the route on the interface it received it on, but it will mark the route as unreachable. Any unreachable routes are automatically removed from the routing table. This is also called split horizon with poison reverse.

Note: All fields are optional.

Variable	Description	Default
`edit <interface_name>`	Type the name of the FortiGate unit interface that is linked to the RIP network. The interface might be a virtual IPSec or GRE interface.	No default.
`split-horizon {poisoned | regular}`	Configure RIP to use either regular or poisoned split horizon on this interface. Choose one of: **`regular`** — prevent RIP from sending updates for a route back out on the interface from which it received that route. **`poisoned`** — send updates with routes learned on an interface back out the same interface but mark those routes as unreachable.	`poisoned`
`split-horizon-status {enable | disable}`	Enable or disable split horizon for this interface. Split horizon is enabled by default. Disable split horizon only if there is no possibility of creating a counting to infinity loop when network topology changes.	`enable`

config neighbor

Use this subcommand to enable RIPng to send unicast routing updates to the router at the specified address. You can use the `neighbor` subcommand and “passive-interface <name_str>” on page 341 to allow RIPng to send unicast updates to the specified neighbor while blocking broadcast updates on the specified interface. You can configure multiple neighbors.

Note: All fields are required.

Variable	Description	Default
`edit <neighbor_id>`	Enter an entry number for the RIPng neighbor. The number must be an integer.	No default.
`interface <name>`	The interface that connects to the neighbor.	No default.
`ip6 <address_ipv6>`	Enter the IP address of the neighboring router to which to send unicast updates.	`::`

config offset-list

Use this subcommand to add the specified offset to the metric (hop count) of a route from the offset list.

Note: The `access-list6`, `direction`, and `offset` fields are required. All other fields are optional.

Variable	Description	Default
`edit <offset_list_id>`	Enter an entry number for the offset list. The number must be an integer.	No default.
`access-list6 <name_str>`	Enter the name of the access list to use for this offset list. The access list is used to determine which routes to add the metric to.	`Null.`
`direction {in | out}`	Enter `in` to apply the offset to the metrics of incoming routes. Enter `out` to apply the offset to the metrics of outgoing routes.	`out`
`interface <name_str>`	Enter the name of the interface to match for this offset list.	`Null.`
`offset <metric_integer>`	Enter the offset number to add to the metric. The metric is the hop count. The `metric_integer` range is from 1 to 16, with 16 being unreachable.	`0`
`status {enable | disable}`	Enable or disable this offset list.	`disable`

config redistribute

Use this subcommand to redistribute routes learned from OSPF, BGP, static routes, or a direct connection to the destination network.

The RIPng redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- `bgp` — Redistribute routes learned from BGP.
- `connected` — Redistribute routes learned from a direct connection to the destination network.
- `ospf` — Redistribute routes learned from OSPF.
- `static` — Redistribute the static routes defined in the FortiGate unit routing table.

When you enter the subcommand, end the command with one of the four static entry names (that is, `config redistribute {bgp | connected | ospf | static}`).

Note: All fields are optional.

Variable	Description	Default
`metric <metric_integer>`	Enter the metric value to be used for the redistributed routes. The `metric_integer` range is from 0 to 16.	`0`
`routemap <name_str>`	Enter the name of the route map to use for the redistributed routes.	`Null.`
`status {enable | disable}`	Enable or disable redistributing routes.	`disable`

History

FortiOS v4.0 MR1 New.

Related topics

- router access-list, access-list6
- router prefix-list, prefix-list6
- router rip
- router route-map

route-map

Use this command to add, edit, or delete route maps. To use the command to limit the number of received or advertised BGP and RIP routes and routing updates using route maps, see “Using route maps with BGP” on page 356, and RIP “config redistribute” on page 326.

Route maps provide a way for the FortiGate unit to evaluate optimum routes for forwarding packets or suppressing the routing of packets to particular destinations. Compared to access lists, route maps support enhanced packet-matching criteria. In addition, route maps can be configured to permit or deny the addition of routes to the FortiGate unit routing table and make changes to routing information dynamically as defined through route-map rules.

The FortiGate unit compares the rules in a route map to the attributes of a route. The rules are examined in ascending order until one or more of the rules in the route map are found to match one or more of the route attributes:

- When a single matching `match-*` rule is found, changes to the routing information are made as defined through the rule’s `set-ip-nexthop`, `set-metric`, `set-metric-type`, and/or `set-tag` settings.
- If no matching rule is found, no changes are made to the routing information.
- When more than one `match-*` rule is defined, all of the defined `match-*` rules must evaluate to TRUE or the routing information is not changed.
- If no `match-*` rules are defined, the FortiGate unit makes changes to the routing information only when all of the default `match-*` rules happen to match the attributes of the route.

The default rule in the route map (which the FortiGate unit applies last) denies all routes. For a route map to take effect, it must be called by a FortiGate unit routing process.

Note: Any fields and rules that to not appear here can be found in the BGP route-map section. See “Using route maps with BGP” on page 356.

Syntax

```
config router route-map
  edit <route_map_name>
    set comments <string>
    config rule
    edit <route_map_rule_id>
      set action {deny | permit}
      set match-interface <name_str>
      set match-ip-address <access/prefix-listname_str>
      set match-ip-nexthop <access/prefix-listname_str>
      set match-metric <metric_integer>
      set match-route-type {1 | 2}
      set match-tag <tag_integer>
      set set-ip-nexthop <address_ipv4>
      set set-metric <metric_integer>
      set set-metric-type {1 | 2}
      set set-tag <tag_integer>
    end
  end
```

Note: All fields are optional.

Variable	Description	Default
edit <route_map_name>	Enter a name for the route map.	No default.
comments <string>	Enter a description for this route map name.	No default.
config rule variables		
edit <route_map_rule_id>	Enter an entry number for the rule. The number must be an integer.	No default.
action {deny | permit}	Enter permit to permit routes that match this rule. Enter deny to deny routes that match this rule.	permit
match-interface <name_str>	Enter the name of the local FortiGate unit interface that will be used to match route interfaces.	Null.
match-ip-address <access/prefix-listname_str>	Match a route if the destination address is included in the specified access list or prefix list.	Null.
match-ip6-address <access/prefix-listname_str>	Match a route if the destination IPv6 address is included in the specified access6 list or prefix6 list.	Null.
match-ip-nexthop <access/prefix-listname_str>	Match a route that has a next-hop router address included in the specified access list or prefix list.	Null.
match-ip6-nexthop <access/prefix-listname_str>	Match a route that has a next-hop router address included in the specified access6 list or prefix6 list.	Null.
match-metric <metric_integer>	Match a route with the specified metric. The metric can be a number from 1 to 16.	0
match-route-type {1 | 2}	Match a route that has the external type set to 1 or 2.	external-type1
match-tag <tag_integer>	This field is available when set-tag is set. Match a route that has the specified tag.	0
set-ip-nexthop <address_ipv4>	Set the next-hop router address for a matched route.	0.0.0.0
set-ip6-nexthop <address_ipv6>	Set the next-hop router IPv6 address for a matched route.	::0
set-ip6-nexthop-local <address_ipv6>	Set the next-hop router local IPv6 address for a matched route.	::0
set-metric <metric_integer>	Set a metric value of 1 to 16 for a matched route.	0
set-metric-type {1 | 2}	Set the type for a matched route.	external-type1
set-tag <tag_integer>	Set a tag value for a matched route.	0

Example

This example shows how to add a route map list named rtmp2 with two rules. The first rule denies routes that match the IP addresses in an access list named acc_list2. The second rule permits routes that match a metric of 2 and changes the metric to 4.

```
config router route-map
  edit rtmp2
  config rule
    edit 1
      set match-ip-address acc_list2
      set action deny
    next
    edit 2
      set match-metric 2
      set action permit
      set set-metric 4
    end
```

```
end
```

Using route maps with BGP

When a connection is established between BGP peers, the two peers exchange all of their BGP route entries. Afterward, they exchange updates that only include changes to the existing routing information. Several BGP entries may be present in a route-map table. You can limit the number of received or advertised BGP route and routing updates using route maps. Use the `config router route-map` command to create, edit, or delete a route map.

Note: When you specify a route map for the `dampening-route-map` value through the `config router bgp` command (see "dampening-route-map <routemap-name_str>" on page 287), the FortiGate unit ignores global dampening settings. You cannot set global dampening settings for the FortiGate unit and then override those values through a route map.

Syntax

```
config router route-map
  edit <route_map_name>
    set comments <string>
    config rule
    edit <route_map_rule_id>
      set match-as-path <aspath-list-name_str>
      set match-community <community-list-name_str>
      set match-community-exact {enable | disable}
      set match-origin {egp | igp |  incomplete | none}
      set set-aggregator-as <id_integer>
      set set-aggregator-ip <address_ipv4>
      set set-aspath <id_integer> <id_integer> <id_integer> ...
      set set-atomic-aggregate {enable | disable}
      set set-community-delete <community-list-name_str>
      set set-community <criteria>
      set set-community-additive {enable | disable}
      set set-dampening-reachability-half-life <minutes>
      set set-dampening-reuse <reuse_integer>
      set set-dampening-suppress <suppress_integer>
      set set-dampening-max-suppress <minutes>
      set set-dampening-unreachability-half-life <minutes>
      set set-extcommunity-rt <AA:NN> <AA:NN> <AA:NN> ...
      set set-extcommunity-soo <AA:NN> <AA:NN> <AA:NN> ...
      set set-local-preference <preference_integer>
      set set-originator-id <address_ipv4>
      set set-origin {egp | igp | incomplete | none}
      set set-weight <weight_integer>
    end
```

Note: All fields are optional.

Variable	Description	Default
`edit <route_map_name>`	Enter a name for the route map.	No default.
`comments <string>`	Enter a description for this route map name.	No default.
config rule variables		
`edit <route_map_rule_id>`	Enter an entry number for the rule. The number must be an integer.	No default.

Variable	Description	Default
`match-as-path <aspath-list-name_str>`	Enter the AS-path list name that will be used to match BGP route prefixes. You must create the AS-path list before it can be selected here. See “aspath-list” on page 279.	`Null.`
`match-community <community-list-name_str>`	Enter the community list name that will be used to match BGP routes according to their COMMUNITY attributes. You must create the community list before it can be selected here. See “community-list” on page 299.	`Null.`
`match-community-exact {enable | disable}`	This field is only available when `match-community` is set. Enable or disable an exact match of the BGP route community specified by the `match-community` field.	`disable`
`match-origin {egp | igp | incomplete | none}`	Enter a value to compare to the ORIGIN attribute of a routing update: **egp** — set the value to the NLRI learned from the Exterior Gateway Protocol (EGP). The FortiGate unit has the second-highest preference for routes of this type. **igp** — set the value to the NLRI learned from a protocol internal to the originating AS. The FortiGate unit has the highest preference for routes learned through Internal Gateway Protocol (IGP). **incomplete** — match routes that were learned some other way (for example, through redistribution). **none** — disable the matching of BGP routes based on the origin of the route.	`none`
`set-aggregator-as <id_integer>`	Set the originating AS of an aggregated route. The value specifies at which AS the aggregate route originated. The range is from 1 to 65 535. The `set-aggregator-ip` value must also be set to further identify the originating AS.	unset
`set-aggregator-ip <address_ipv4>`	This field is available when `set-aggregator-as` is set. Set the IP address of the BGP router that originated the aggregate route. The value should be identical to the FortiGate unit `router-id` value (see “`router-id <address_ipv4>`” on page 288).	`0.0.0.0`
`set-aspath <id_integer> <id_integer> <id_integer> ...`	Modify the FortiGate unit AS_PATH attribute and add to it the AS numbers of the AS path belonging to a BGP route. The resulting path describes the autonomous systems along the route to the destination specified by the NLRI. The range is from 1 to 65 535. The `set-aspath` value is added to the beginning of the AS_SEQUENCE segment of the AS_PATH attribute of incoming routes, or to the end of the AS_SEQUENCE segment of the AS_PATH attribute of outgoing routes. Enclose all AS numbers in quotes if there are multiple occurrences of the same id_integer. Otherwise the AS path may be incomplete.	No default.
`set-atomic-aggregate {enable | disable}`	Enable or disable a warning to upstream routers through the ATOMIC_AGGREGATE attribute that address aggregation has occurred on an aggregate route. This value does not have to be specified when an `as-set` value is specified in the aggregate-address table (see “config aggregate-address” on page 289).	`disable`
`set-community-delete <community-list-name_str>`	Remove the COMMUNITY attributes from the BGP routes identified in the specified community list. You must create the community list first before it can be selected here (see “community-list” on page 299).	`Null.`

Variable	Description	Default
`set-community <criteria>`	Set the COMMUNITY attribute of a BGP route. • Use decimal notation to set a specific COMMUNITY attribute for the route. The value has the syntax `AA:NN`, where `AA` represents an AS, and `NN` is the community identifier. Delimit complex expressions with double-quotation marks (for example, `"123:234 345:456"`). • To make the route part of the Internet community, select `internet`. • To make the route part of the LOCAL_AS community, select `local-AS`. • To make the route part of the NO_ADVERTISE community, select `no-advertise`. • To make the route part of the NO_EXPORT community, select `no-export`.	No default.
`set-community-additive {enable | disable}`	This field is available when `set-community` is set. Enable or disable the appending of the `set-community` value to a BGP route.	`disable`
`set-dampening-reachability-half-life <minutes>`	Set the dampening reachability half-life of a BGP route (in minutes). The range is from 1 to 45.	`0`
`set-dampening-reuse <reuse_integer>`	Set the value at which a dampened BGP route will be reused. The range is from 1 to 20 000. If you set `set-dampening-reuse`, you must also set `set-dampening-suppress` and `set-dampening-max-suppress`.	`0`
`set-dampening-suppress <suppress_integer>`	Set the limit at which a BGP route may be suppressed. The range is from 1 to 20 000. See also "`dampening-suppress <limit_integer>`" on page 287.	`0`
`set-dampening-max-suppress <minutes>`	Set maximum time (in minutes) that a BGP route can be suppressed. The range is from 1 to 255. See also "`dampening-max-suppress-time`" in "`dampening-max-suppress-time <minutes_integer>`" on page 287.	`0`
`set-dampening-unreachability-half-life <minutes>`	Set the unreachability half-life of a BGP route (in minutes). The range is from 1 to 45. See also "`dampening-unreachability-half-life <minutes_integer>`" on page 287.	`0`
`set-extcommunity-rt <AA:NN> <AA:NN> <AA:NN> ...`	Set the target extended community (in decimal notation) of a BGP route. The COMMUNITY attribute value has the syntax `AA:NN`, where `AA` represents an AS, and `NN` is the community identifier.	No default.
`set-extcommunity-soo <AA:NN> <AA:NN> <AA:NN> ...`	Set the site-of-origin extended community (in decimal notation) of a BGP route. The COMMUNITY attribute value has the syntax `AA:NN`, where `AA` represents an AS, and `NN` is the community identifier.	No default.
`set-local-preference <preference_integer>`	Set the LOCAL_PREF value of an IBGP route. The value is advertised to IBGP peers. The range is from 0 to 4 294 967 295. A higher number signifies a preferred route among multiple routes to the same destination.	`0`
`set-originator-id <address_ipv4>`	Set the ORIGINATOR_ID attribute, which is equivalent to the `router-id` of the originator of the route in the local AS. Route reflectors use this value to prevent routing loops.	`0.0.0.0`

Variable	Description	Default
set-origin {egp | igp | incomplete | none}	Set the ORIGIN attribute of a local BGP route. Choose one of: **egp** — set the value to the NLRI learned from the Exterior Gateway Protocol (EGP). **igp** — set the value to the NLRI learned from a protocol internal to the originating AS. **incomplete** — if not egp or igp. **none** — disable the ORIGIN attribute.	none
set-weight <weight_integer>	Set the weight of a BGP route. A route's weight has the most influence when two identical BGP routes are compared. A higher number signifies a greater preference. The range is from 0 to 2 147 483 647.	0

Example

This example shows how to create a route map named BGP_rtmp2. The route map contains two rules. The first rule permits operations on routes that match the IP addresses in an access list named acc_list2. The second rule permits operations on routes according to a community list named com_list3.

```
config router route-map
  edit BGP_rtmp2
    set comments “example BGP route map”
    config rule
    edit 1
      set match-ip-address acc_list2
      set action permit
    next
    edit 2
      set match-community com_list3
      set action permit
    end
  end
```

History

FortiOS v2.80	New.
FortiOS v3.0	Added support for BGP.
FortiOS v3.0 MR6	Added comments field.
FortiOS v4.0 MR1	Added match-ip6-address, match-ip6-nexthop, set-ip6-nexthop, and set-ip6-nexthop-local.

Related topics

- router access-list, access-list6
- router prefix-list, prefix-list6
- router rip
- router aspath-list
- router bgp
- router community-list
- router key-chain

setting

Use this command to define a prefix list as a filter to show routes.

Command

```
config router setting
  set show-filter <prefix_list>
end
```

History

FortiOS v4.0 New.

Related topics

- router prefix-list, prefix-list6

static

Use this command to add, edit, or delete static routes for IPv4 traffic. For IPv6 traffic, use the `static6` command at "static6" on page 364.

You add static routes to manually control traffic exiting the FortiGate unit. You configure routes by specifying destination IP addresses and network masks and adding gateways for these destination addresses. Gateways are the next-hop routers to which traffic that matches the destination addresses in the route are forwarded.

You can adjust the administrative distance of a route to indicate preference when more than one route to the same destination is available. The lower the administrative distance, the greater the preferability of the route. If the routing table contains several entries that point to the same destination (the entries may have different gateways or interface associations), the FortiGate unit compares the administrative distances of those entries, selects the entries having the lowest distances, and installs them as routes in the FortiGate unit forwarding table. Any ties are resolved by comparing the routes' priority, with lowest priority being preferred. As a result, the FortiGate unit forwarding table only contains routes having the lowest distances to every possible destination.If both administrative distance and priority are tied for two or more routes, an equal cost multi-path (ECMP) situation occurs. In this case, the egress index for the routes will be used to determine the selected route.

Syntax

```
config router static
  edit <sequence_number>
    set blackhole {enable | disable}
    set device <interface_name>
    set distance <distance>
    set dst <destination-address_ipv4mask>
    set dynamic-gateway {enable | disable}
    set gateway <gateway-address_ipv4>
    set priority <integer>
    set weight <integer>
  end
```

Note: The `dst` and `gateway` fields are required when `blackhole` is disabled. When `blackhole` is enabled, the `dst` field is required. All other fields are optional.

Variable	Description	Default
`edit <sequence_number>`	Enter a sequence number for the static route. The sequence number may influence routing priority in the FortiGate unit forwarding table.	No default.
`blackhole {enable | disable}`	Enable or disable dropping all packets that match this route. This route is advertised to neighbors through dynamic routing protocols as any other static route.	`disable`
`device <interface_name>`	This field is available when `blackhole` is set to `disable`. Enter the name of the FortiGate unit interface through which to route traffic. Use '?' to see a list of interfaces.	`Null.`
`distance <distance>`	Enter the administrative distance for the route. The distance value may influence route preference in the FortiGate unit routing table. The range is an integer from 1-255. See also config system interface "distance <distance_integer>" on page 259.	`10`

Variable	Description	Default
dst <destination-address_ipv4mask>	Enter the destination IPv4 address and network mask for this route. You can enter 0.0.0.0 0.0.0.0 to create a new static default route.	0.0.0.0 0.0.0.0
dynamic-gateway {enable | disable}	When enabled, dynamic-gateway hides the gateway variable for a dynamic interface, such as a DHCP or PPPoE interface. When the interface connects or disconnects, the corresponding routing entries are updated to reflect the change.	disable
gateway <gateway-address_ipv4>	This field is available when blackhole is set to disable. Enter the IPv4 address of the next-hop router to which traffic is forwarded.	0.0.0.0
priority <integer>	The administrative priority value is used to resolve ties in route selection. In the case where both routes have the same priority, such as equal cost multi-path (ECMP), the egress index for the routes will be used to determine the selected route. The range is an integer from 0 to 4294967295. Lower priority routes are preferred routes. This field is only accessible through the CLI.	0
weight <integer>	Add weights to ECMP static routes if the ECMP route failover and load balance method is set to weighted. Enter weights for ECMP routes. More traffic is directed to routes with higher weights. This option is available when the v4-ecmp-mode field of the config system settings command is set to weight-based. For more information, see "system settings" on page 517.	0

Example

This example shows how to add a static route that has the sequence number 2.

```
config router static
  edit 2
    set dev internal
    set dst 192.168.22.0 255.255.255.0
    set gateway 192.168.22.44
  end
```

This example shows how to add a static route for a dynamic modem interface with a administrative distance of 1 and a priority of 1. These settings makes this the preferred route.

```
config route static
  edit 3
    set dev modem
    set dynamic-gateway enable
    set dst 10.0.0.7 255.255.255.0
    set distance 1
    set priority 1
  end
```

History

FortiOS v2.80 Substantially revised.

FortiOS v3.0 Added blackhole attribute.

FortiOS v3.0 MR2 Added dynamic-gateway attribute.

FortiOS v3.0 MR6 Added default value for priority.

FortiOS 4.0 MR1 Added weight field.

Related topics

- system interface
- system settings
- get router info routing-table

static6

Use this command to add, edit, or delete static routes for IPv6 traffic. For IPv4 static routes, see “static” on page 361.

You add static routes to specify the destination of traffic exiting the FortiGate unit. You configure routes by adding destination IP addresses and network masks and adding gateways for these destination addresses. The gateways are the next-hop routers to which traffic that matches the destination addresses in the route are forwarded.

Note: You can configure static routes for IPv6 traffic on FortiGate units that run in NAT/Route mode.

Syntax

```
config router static6
  edit <sequence_number>
    set device <interface_name>
    set dst <destination-address_ipv6mask>
    set gateway <gateway-address_ipv6>
  end
```

Note: The `device`, `dst`, and `gateway` fields are all required.

Variable	Description	Default
`edit <sequence_number>`	Enter a sequence number for the static route.	No default.
`device <interface_name>`	The name of the FortiGate unit interface through which to route traffic.	`Null.`
`dst <destination-address_ipv6mask>`	The destination IPv6 address and netmask for this route. You can enter `::/0` to create a new static default route for IPv6 traffic.	`::/0`
`gateway <gateway-address_ipv6>`	The IPv6 address of the next-hop router to which traffic is forwarded.	`::`

Example

This example shows how to add an IPv6 static route that has the sequence number 2.

```
config router static6
  edit 2
    set dev internal
    set dst 2001:DB8::/32
    set gateway 2001:DB8:0:CD30:123:4567:89AB:CDEF
  end
```

History

FortiOS v2.80 New.

Related topics

- system interface
- get router info routing-table

spamfilter

Use email filter commands to create a banned word list, configure filters based on email addresses, ip addresses, and MIME headers, and to configure the FortiGuard-Antispam service.

For more information about email filtering see the *FortiGate UTM User Guide*.

This chapter contains the following sections:

bword

Use this command to add or edit and configure options for the email filter banned word list.

The FortiGate email filters are applied in the following order:

For SMTP

1 IP address BWL check - Last hop IP
2 DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3 E-mail address BWL check
4 MIME headers check
5 IP address BWL check (for IPs extracted from “Received” headers)
6 Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7 Banned word check

For POP3 and IMAP

1 E-mail address BWL check
2 MIME headers check, IP BWL check
3 Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4 Banned word check

For SMTP, POP3, and IMAP

Control spam by blocking email messages containing specific words or patterns. If enabled in the protection profile, the FortiGate unit searches for words or patterns in email messages. If matches are found, values assigned to the words are totalled. If a user-defined threshold value is exceeded, the message is marked as spam. If no match is found, the email message is passed along to the next filter.

Use Perl regular expressions or wildcards to add banned word patterns to the list. Add one or more banned words to sort email containing those words in the email subject, body, or both. Words can be marked as spam or clear. Banned words can be one word or a phrase up to 127 characters long.

If a single word is entered, the FortiGate unit blocks all email that contain that word. If a phrase is entered, the FortiGate unit blocks all email containing the exact phrase. To block any word in a phrase, use Perl regular expressions.

Note: Perl regular expression patterns are case sensitive for email filter banned words. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` blocks all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

Syntax

```
config spamfilter bword
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
    config entries
      edit <banned_word_int>
        set action {clear | spam}
        set language {french | japanese | korean | simch | spanish | thai |
            trach | western}
        set pattern <banned_word_str>
```

```
    set pattern-type {regexp | wildcard}
    set score <int>
    set status {enable | disable}
    set where {all | body | subject}
  end
```

Variable	Description	Default
<list_int>	A unique number to identify the banned word list.	
<list_str>	The name of the banned word list.	
<comment_str>	The comment attached to the banned word list.	
<banned_word_int>	A unique number to identify the banned word or pattern.	
action {clear | spam}	Enter clear to allow the email. Enter spam to apply the spam action configured in the protection profile.	spam
language {french | japanese | korean | simch | spanish | thai | trach | western}	Enter the language character set used for the banned word or phrase. Choose from French, Japanese, Korean, Simplified Chinese, Thai, Traditional Chinese, or Western.	western
pattern <banned_word_str>	Enter the banned word or phrase pattern using regular expressions or wildcards.	No default.
pattern-type {regexp | wildcard}	Enter the pattern type for the banned word (pattern). Choose from regular expressions or wildcard.	wildcard
score <int>	A numerical weighting applied to the banned word. The score values of all the matching words appearing in an email message are added, and if the total is greater than the spamwordthreshold value set in the protection profile, the message is processed according to the spam action setting in the protection profile. The score for a banned word is counted once even if the word appears multiple times in an email message.	10
status {enable | disable}	Enable or disable scanning email for each banned word.	enable
where {all | body | subject}	Enter where in the email to search for the banned word or phrase.	all

History

FortiOS v2.80	New.
FortiOS v2.80 MR2	Added French and Thai variables to the language field.
FortiOS v3.0	Added score variable. Added multiple-list capability for models 800 and above.
FortiOS v3.0 MR4	All models have the same CLI syntax now.
FortiOS v4.0	Added the spanish option to the available languages.

Related topics

- spamfilter emailbwl
- spamfilter fortishield
- spamfilter ipbwl
- spamfilter iptrust
- spamfilter mheader
- spamfilter options
- spamfilter dnsbl

dnsbl

Use this command to configure email filtering using DNS-based Blackhole List (DNSBL) or Open Relay Database List (ORDBL) servers. DSNBL and ORDBL settings are configured with this command but DSNBL and ORDBL filtering is enabled within each protection profile.

The FortiGate email filters are generally applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP

The FortiGate unit compares the IP address or domain name of the sender to any database lists configured in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next email filter.

Some spammers use unsecured third party SMTP servers to send unsolicited bulk email. Using DNSBLs and ORDBLs is an effective way to tag or reject spam as it enters the network. These lists act as domain name servers that match the domain of incoming email to a list of IP addresses known to send spam or allow spam to pass through.

There are several free and subscription servers available that provide reliable access to continually updated DNSBLs and ORDBLs. Please check with the service being used to confirm the correct domain name for connecting to the server.

Note: Because the FortiGate unit uses the server domain name to connect to the DNSBL or ORDBL server, it must be able to look up this name on the DNS server. For information on configuring DNS, see “system dns” on page 413.

Syntax

```
config spamfilter dnsbl
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
    config entries
      edit <server_int>
        set action {reject | spam}
        set server <fqdn>
```

```
    set status {enable | disable}
end
```

Variable	Description	Default
<list_int>	A unique number to identify the DNSBL list.	
<list_str>	The name of the DNSBL header list.	
<comment_str>	The comment attached to the DNSBL header list.	
<server_int>	A unique number to identify the DNSBL server.	
action {reject | spam}	Enter reject to stop any further processing of the current session and to drop an incoming connection at once. Enter spam to identify email as spam.	spam
server <fqdn>	Enter the domain name of a DNSBL server or an ORDBL server.	No default.
status {enable | disable}	Enable or disable querying the server named in the server string.	enable

History

FortiOS v2.80	New.
FortiOS v3.0	Added multiple-list capability for models 800 and above.
FortiOS v3.0 MR2	Multiple-list feature is available for all models.
FortiOS v3.0 MR5	Changed RBL to DNSBL.

Related topics

- spamfilter bword
- spamfilter emailbwl
- spamfilter fortishield
- spamfilter ipbwl
- spamfilter iptrust
- spamfilter mheader
- spamfilter options
- system dns

emailbwl

Use this command to filter email based on the sender's email address or address pattern.

The FortiGate email filters are applied in the following order:

For SMTP

1 IP address BWL check - Last hop IP
2 DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3 E-mail address BWL check
4 MIME headers check
5 IP address BWL check (for IPs extracted from "Received" headers)
6 Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from "Received" headers, and URLs in email content)
7 Banned word check

For POP3 and IMAP

1 E-mail address BWL check
2 MIME headers check, IP BWL check
3 Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4 Banned word check

For SMTP, POP3, and IMAP

The FortiGate unit uses the email address list to filter incoming email. The FortiGate unit compares the email address or domain of the sender to the list in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next email filter.

The FortiGate unit can filter email from specific senders or all email from a domain (such as example.net). Each email address can be marked as clear or spam.

Use Perl regular expressions or wildcards to add email address patterns to the list.

Syntax

```
config spamfilter emailbwl
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
    config entries
      edit <email_int>
        set action {clear | spam}
        set email-pattern <email_str>
        set pattern-type {regexp | wildcard}
        set status {enable | disable}
      end
```

Variable	Description	Default
<list_int>	A unique number to identify the email black/white list.	
<list_str>	The name of the email black/white list.	
<comment_str>	The comment attached to the email black/white list.	

Variable	Description	Default
<email_int>	A unique number to identify the email pattern.	
action {clear | spam}	Enter clear to exempt the email from the rest of the spam filters. Enter spam to apply the spam action configured in the protection profile.	spam
email-pattern <email_str>	Enter the email address pattern using wildcards or Perl regular expressions.	
pattern-type {regexp | wildcard}	Enter the pattern-type for the email address. Choose from wildcards or Perl regular expressions.	wildcard
status {enable | disable}	Enable or disable scanning for each email address.	enable

History

FortiOS v2.80 New.

FortiOS v3.0 Added multiple-list capability for models 800 and above.

FortiOS v3.0 MR4 All models have the same CLI syntax now.

Related topics

- spamfilter bword
- spamfilter fortishield
- spamfilter ipbwl
- spamfilter iptrust
- spamfilter mheader
- spamfilter options
- spamfilter dnsbl

fortishield

Use this command to configure the settings for the FortiGuard-Antispam Service.

The FortiGate email filters are applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP

FortiGuard-Antispam Service is an antispam system from Fortinet that includes an IP address black list, a URL black list, and email filtering tools. The IP address black list contains IP addresses of email servers known to be used to generate Spam. The URL black list contains found in Spam email.

FortiGuard-Antispam Service compiles the IP address and URL list from email captured by spam probes located around the world. Spam probes are email addresses purposely configured to attract spam and identify known spam sources to create the antispam IP address and URL list. FortiGuard-Antispam Service combines IP address and URL checks with other email filter techniques in a two-pass process.

On the first pass, if `spamfsip` is selected in the protection profile, FortiGuard-Antispam Service extracts the SMTP mail server source address and sends the IP address to a FortiGuard-Antispam Service server to see if this IP address matches the list of known spammers. If `spamfsurl` is selected in the protection profile, FortiGuard-Antispam Service checks the body of email messages to extract any URL links. These URL links will be sent to a FortiGuard-Antispam Service server to see if any of them is listed. Typically spam messages contain URL links to advertisements (also called spamvertizing).

If an IP address or URL match is found, FortiGuard-Antispam Service terminates the session. If FortiGuard-Antispam Service does not find a match, the mail server sends the email to the recipient.

As each email is received, FortiGuard-Antispam Service performs the second antispam pass by checking the header, subject, and body of the email for common spam content. If FortiGuard-Antispam Service finds spam content, the email is tagged or dropped according to the configuration in the firewall protection profile.

Both FortiGuard-Antispam Service antispam processes are completely automated and configured by Fortinet. With constant monitoring and dynamic updates, FortiGuard-Antispam Service is always current. Enable or disable FortiGuard-Antispam Service in a firewall protection profile.

Syntax

```
config spamfilter fortishield
  set reports-status {enable | disable}
  set spam-submit-force {enable | disable}
  set spam-submit-srv <url_str>
  set spam-submit-txt2htm {enable | disable}
end
```

Variable	Description	Default
`reports-status {enable | disable}`	Enable to have the FortiGate unit maintain FortiGuard Antispam statistics. These statistics will be compiled only on FortiGate units equipped with a hard drive. View these statistics with the `diagnose spamfilter fortishield report` command.	`enable`
`spam-submit-force {enable | disable}`	Enable or disable force insertion of a new mime entity for the submission text.	`enable`
`spam-submit-srv <url_str>`	The host name of the FortiGuard-Antispam Service server. The FortiGate unit comes preconfigured with the host name. Use this command only to change the host name.	www.nospammer.net
`spam-submit-txt2htm {enable | disable}`	Enable or disable converting text email to HTML.	enable

History

FortiOS v2.80 MR7	New.
FortiOS v3.0	Some revisions and added `port` and `timeout`.
FortiOS v3.0 MR1	Restructured -- some commands were moved to `system fortiguard` and some new commands were added.
FortiOS 4.0.0	Added the `reports-status` command.

Related topics

- spamfilter bword
- spamfilter emailbwl
- spamfilter ipbwl
- spamfilter iptrust
- spamfilter mheader
- spamfilter options
- spamfilter dnsbl

ipbwl

Use this command to filter email based on the IP or subnet address.

The FortiGate email filters are generally applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP

The FortiGate unit uses the IP address list to filter incoming email. The FortiGate unit compares the IP address of the sender to the list in sequence. If a match is found, the corresponding protection profile action is taken. If no match is found, the email is passed on to the next email filter.

Enter an IP address and mask in one of two formats:

- x.x.x.x/x.x.x.x, for example 192.168.10.23/255.255.255.0
- x.x.x.x/x, for example 192.168.10.23/24

Configure the FortiGate unit to filter email from specific IP addresses. Mark each IP address as clear, spam, or reject. Filter single IP addresses, or a range of addresses at the network level by configuring an address and mask.

Syntax

```
config spamfilter ipbwl
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
    config entries
       edit <address_int>
        set action {clear | reject | spam}
        set addr-type {ipv4 | ipv6}
        set ip4-subnet {<address_ipv4mask>}
        set ip6-subnet {<address_ipv6mask>}
        set status {enable | disable}
      end
```

Variable	Description	Default
<list_int>	A unique number to identify the IP black/white list.	
<list_str>	The name of the IP black/white list.	
<comment_str>	The comment attached to the IP black/white list.	
<address_int>	A unique number to identify the address.	
action {clear | reject | spam}	Enter clear to exempt the email from the rest of the email filters. Enter reject to drop any current or incoming sessions. Enter spam to apply the spam action configured in the protection profile.	spam
addr-type {ipv4 | ipv6}	Select whether IPv4 or IPv6 addresses will be used.	ipv4
ip4-subnet {<address_ipv4mask>}	The trusted IPv4 IP address and subnet mask in the format 192.168.10.23 255.255.255.0 or 192.168.10.23/24.	No default
ip6-subnet {<address_ipv6mask>}	The trusted IPv6 IP address. This is available when addr-type is ipv6.	No default
status {enable | disable}	Enable or disable scanning email for each IP address.	enable

History

FortiOS v2.80 New.

FortiOS v3.0 Added multiple-list capability for models 800 and above.

FortiOS v3.0 MR4 All models have the same CLI syntax now.

FortiOS v4.0 MR1 ip/subnet replaced by ip4-subnet and ip6-subnet. Added addr-type.

Related topics

- spamfilter bword
- spamfilter emailbwl
- spamfilter fortishield
- spamfilter iptrust
- spamfilter mheader
- spamfilter options
- spamfilter dnsbl

iptrust

Use this command to add an entry to a list of trusted IP addresses.

If the FortiGate unit sits behind a company's Mail Transfer Units, it may be unnecessary to check email IP addresses because they are internal and trusted. The only IP addresses that need to be checked are those from outside of the company. In some cases, external IP addresses may be added to the list if it is known that they are not sources of spam.

Syntax

```
config spamfilter iptrust
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
    config entries
      edit <address_int>
        set addr-type {ipv4 | ipv6}
        set ip4-subnet {<address_ipv4mask>}
        set ip6-subnet {<address_ipv6mask>}
        set status {enable | disable}
      end
```

Variable	Description	Default
`addr-type {ipv4 | ipv6}`	Select whether IPv4 or IPv6 addresses will be used.	`ipv4`
`<list_int>`	A unique number to identify the IP trust list.	
`<list_str>`	The name of the IP trust list.	
`<comment_str>`	The comment attached to the IP trust list.	
`<address_int>`	A unique number to identify the address.	
`ip4-subnet {<address_ipv4mask>}`	The trusted IPv4 IP address and subnet mask in the format `192.168.10.23 255.255.255.0` or `192.168.10.23/24`.	No default
`ip6-subnet {<address_ipv6mask>}`	The trusted IPv6 IP address. This is available when `addr-type` is `ipv6`.	No default
`status {enable | disable}`	Enable or disable the IP address.	`enable`

History

FortiOS v3.0 New.

FortiOS v3.0 MR4 All models have the same CLI syntax now.

FortiOS v4.0 MR1 `ip/subnet` replaced by `ip4-subnet` and `ip6-subnet`. Added `addr-type`.

Related topics

- spamfilter bword, spamfilter emailbwl
- spamfilter fortishield
- spamfilter ipbwl
- spamfilter mheader
- spamfilter options
- spamfilter dnsbl

mheader

Use this command to configure email filtering based on the MIME header. MIME header settings are configured with this command but MIME header filtering is enabled within each protection profile.

The FortiGate email filters are applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP

The FortiGate unit compares the MIME header key-value pair of incoming email to the list pair in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next email filter.

MIME (Multipurpose Internet Mail Extensions) headers are added to email to describe content type and content encoding, such as the type of text in the email body or the program that generated the email. Some examples of MIME headers include:

- X-mailer: outgluck
- X-Distribution: bulk
- Content_Type: text/html
- Content_Type: image/jpg

The first part of the MIME header is called the header key, or just header. The second part is called the value. Spammers often insert comments into header values or leave them blank. These malformed headers can fool some spam and virus filters.

Use the MIME headers list to mark email from certain bulk mail programs or with certain types of content that are common in spam messages. Mark the email as spam or clear for each header configured.

Use Perl regular expressions or wildcards to add MIME header patterns to the list.

Note: MIME header entries are case sensitive.

Syntax

```
config spamfilter mheader
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
    config entries
      edit <mime_int>
        set action {clear | spam}
        set fieldbody <mime_str>
        set fieldname <mime_str>
        set pattern-type {regexp | wildcard}
        set status {enable | disable}
      end
    end
```

Variable	Description	Default
<list_int>	A unique number to identify the MIME header list.	
<list_str>	The name of the MIME header list.	
<comment_str>	The comment attached to the MIME header list.	
<mime_int>	A unique number to identify the MIME header.	
action {clear | spam}	Enter clear to exempt the email from the rest of the email filters. Enter spam to apply the spam action configured in the protection profile.	spam
fieldbody <mime_str>	Enter the MIME header (key, header field body) using wildcards or Perl regular expressions.	No default.
fieldname <mime_str>	Enter the MIME header value (header field name) using wildcards or Perl regular expressions. Do not include a trailing colon.	No default.
pattern-type {regexp | wildcard}	Enter the pattern-type for the MIME header. Choose from wildcards or Perl regular expressions.	wildcard
status {enable | disable}	Enable or disable scanning email headers for the MIME header and header value defined in the fieldbody and fieldname strings.	enable

History

FortiOS v2.80 New.

FortiOS v3.0 Added multiple-list capability for models 800 and above.

FortiOS v3.0 MR4 All models have the same CLI syntax now.

Related topics

- spamfilter bword
- spamfilter fortishield
- spamfilter fortishield
- spamfilter ipbwl
- spamfilter iptrust
- spamfilter options
- spamfilter dnsbl

options

Use this command to set the spamfilter DNS query timeout.

Syntax

```
config spamfilter options
  set dns-timeout <timeout_int>
end
```

Variable	Description	Default
`dns-timeout <timeout_int>`	Set the DNS query timeout in the range 1 to 30 seconds.	7

Example

This example shows how to set the dns timeout.

```
config spamfilter options
  set dns-timeout 15
end
```

History

FortiOS v3.0 New.

Related topics

- spamfilter bword
- spamfilter emailbwl
- spamfilter fortishield
- spamfilter ipbwl
- spamfilter iptrust
- spamfilter mheader
- spamfilter dnsbl

system

Use `system` commands to configure options related to the overall operation of the FortiGate unit, including:

- Administrative access
- Automatic updating of antivirus and attack definitions
- High availability (HA)
- Network interfaces
- Replacement messages
- VLANs and virtual domains

This chapter contains the following sections:

accprofile

Use this command to add access profiles that control administrator access to FortiGate features. Each FortiGate administrator account must include an access profile. You can create access profiles that deny access, allow read only, or allow both read and write access to FortiGate features.

You cannot delete or modify the super_admin access profile, but you can use the super_admin profile with more than one administrator account.

Syntax

```
config system accprofile
  edit <profile-name>
    set <access-group> <access-level>
    set menu-file <filedata>
    set radius-vdom-override {disable | enable}
    set radius-accprofile-override {disable | enable}
    config fwgrp-permission
      set address {none | read | read-write}
      set others {none | read | read-write}
      set policy {none | read | read-write}
      set profile {none | read | read-write}
      set schedule {none | read | read-write}
      set service {none | read | read-write}
      end
    config loggrp-permission
      set config {none | read | read-write}
      set data-access {none | read | read-write}
    end
    config utmgrp-permission
      set antivirus {none | read | read-write}
      set application-control {none | read | read-write}
      set data-loss-prevention {none | read | read-write}
      set ips {none | read | read-write}
      set spamfilter {none | read | read-write}
      set webfilter {none | read | read-write}
  end
```

Variable	Description		Default
`edit <profile-name>`	Enter a new profile name to create a new profile. Enter an existing profile name to edit that profile.		No default.
`<access-group>`	Enter the feature group for which you are configuring access:		No default.
	`admingrp`	administrator accounts and access profiles	
	`authgrp`	user authentication, including local users, RADIUS servers, LDAP servers, and user groups	
	`endpoint-control-grp`	endpoint control (Endpoint NAC) configuration	
	`fwgrp`	firewall configuration	
`<access-group> (continued)`	`loggrp`	log and report configuration including log settings, viewing logs and alert email settings `execute batch` commands	

Variable	Description		Default
	mntgrp	maintenance commands: reset to factory defaults, format log disk, reboot, restore and shutdown	
	netgrp	interfaces, dhcp servers, zones **get system status** **get system arp table** **config system arp-table** **execute dhcp lease-list** **execute dhcp lease-clear**	No default.
	routegrp	router configuration	
	sysgrp	system configuration except accprofile, admin and autoupdate	
	updategrp	FortiGuard antivirus and IPS updates, manual and automatic	
	utmgrp	UTM configuration	
	vpngrp	VPN configuration	
	wanoptgrp	WAN optimization configuration	
<access-level>	Enter the level of administrator access to this feature:		none
	custom	configures custom access for fwgrp, loggrp or utmgrp access selections only	
	none	no access	
	read	read-only access	
	read-write	read and write access	
config fwgrp-permission fields. Available if fwgrp is set to custom			
address {none | read | read-write}	Enter the level of administrator access to firewall addresses.		none
others {none | read | read-write}	Enter the level of administrator access to virtual IP configurations.		none
policy {none | read | read-write}	Enter the level of administrator access to firewall policies.		none
profile {none | read | read-write}	Enter the level of administrator access to firewall profiles.		none
schedule {none | read | read-write}	Enter the level of administrator access to firewall schedules.		none
service {none | read | read-write}	Enter the level of administrator access to firewall service definitions.		none
config loggrp-permission fields. Available if loggrp is set to custom.			
config {none | read | read-write}	Enter the level of administrator access to the logging configuration.		none
data-access {none | read | read-write}	Enter the level of administrator access to the log data.		none
config utmgrp-permission fields. Available if utmgrp is set to custom.			
antivirus {none | read | read-write}	Enter the level of administrator access to antivirus configuration data.		none
application-control {none | read | read-write}	Enter the level of administrator access to application control data.		none
data-loss-prevention {none | read | read-write}	Enter the level of administrator access to data loss prevention (DLP) data.		none

Variable	Description	Default
ips {none | read | read-write}	Enter the level of administrator access to intrusion prevention (IP) data.	none
spamfilter {none | read | read-write}	Enter the level of administrator access to spamfilter data.	none
webfilter {none | read | read-write}	Enter the level of administrator access to web filter data.	none
menu-file <filedata>	Enter the name of the base64-encoded file of data to configure the menu display on the FortiGate unit.;	none

Examples

Use the following commands to add a new access profile named policy_profile that allows read and write access to firewall policies and that denies access to all other FortiGate features. An administrator account with this access profile can view and edit firewall policies, but cannot view or change any other FortiGate settings or features.

```
config system accprofile
  edit policy_profile
    set fwgrp read-write
  end
```

Use the following commands to add a new access profile named policy_profile_cu that allows customized read and write access to firewall policies and that denies access to all other FortiGate features. An administrator account with this access profile can view and edit the selected custom firewall permissions (address, policy, and schedule), but cannot view or change any other FortiGate settings or features.

```
config system accprofile
  edit policy_profile_cu
    set fwgrp custom
    config fwgrp-permission
      set address read-write
      set policy read-write
      set schedule read-write
    end
  end
end
```

History

FortiOS v2.80	New
FortiOS v3.0 MR1	Removed secgrp feature group.
FortiOS v3.0 MR2	Modifications for super_admin profile and read-write access-level changes (no write only).
FortiOS v3.0 MR4	Modifications for custom fwgrp firewall permissions, execute batch command control assigned to mntgrp (Maintenance) access control group.
FortiOS v3.0 MR6	Added imp2pgrp access profile. Added config fwgrp-permission and config loggrp-permission subcommands.
FortiOS v4.0	Removed avgrp, imp2pgrp and spamgrp from access profiles. Added endpoint-control-grp, utmgrp, and wanoptgrp.
FortiOS v4.0 MR1	Removed ipsgrp and webgrp.

Related topics

- system admin

admin

Use this command to add, edit, and delete administrator accounts. Administrators can control what data modules appear in the FortiGate unit system dashboard by using the `config system admin` command. Administrators must have read and write privileges to make dashboard GUI modifications.

Use the default admin account or an account with system configuration read and write privileges to add new administrator accounts and control their permission levels. Each administrator account except the default admin must include an access profile. You cannot delete the default super admin account or change the access profile (super_admin). In addition, there is also an access profile that allows read-only super admin privileges, super_admin_readonly. The super_admin_readonly profile cannot be deleted or changed, similar to the super_admin profile. This read-only super-admin may be used in a situation where it is necessary to troubleshoot a customer configuration without making changes.

You can authenticate administrators using a password stored on the FortiGate unit or you can use a RADIUS server to perform authentication. When you use RADIUS authentication, you can authenticate specific administrators or you can allow any account on the RADIUS server to access the FortiGate unit as an administrator.

Note: For users with `super_admin` access profile, you can reset the password in the CLI.
For a user ITAdmin with the access profile super_admin, to set the password to 123456:

```
config sys admin
  edit ITAdmin
    set password 123456
  end
```

For a user ITAdmin with the access profile super_admin, to reset the password from 123456 to the default ‘empty’ or ‘null’:

```
config sys admin
  edit ITAdmin
    unset password 123456
  end
```

If you type ‘set password ?’ in the CLI, you will have to enter the new password and the old password in order for the change to be effective. In this case, you will NOT be able to reset the password to ‘empty’ or ‘null’.

You can configure an administrator to only be allowed to log in at certain times. The default setting allows administrators to log in any time.

A vdom/access profile override feature supports authentication of administrators via RADIUS. The admin user will be have access depending on which vdom they are restricted to and their associated access profile. This feature is only available to wildcard admins. There can only be one vdom-override user per system.

For detailed information about configuring administrators, see the System Administration chapter of the FortiGate Administration Guide for your model.

Note: You cannot change the management VDOM if any administrators are using RADIUS authentication.

Syntax

```
config system admin
  edit <name_str>
    set accprofile <profile-name>
    set comments <comments_string>
    set force-password-change {enable | disable}
    set ip6-trusthost1 <address_ipv6mask>
    set ip6-trusthost2 <address_ipv6mask>
```

```
    set ip6-trusthost3 <address_ipv6mask>
    set password <admin_password>
    set password-expire YYYY-MM-DD HH:MM:SS
    set peer-auth {disable | enable}
    set peer-group <peer-grp>
    set radius-accprofile-override {disable | enable}
    set radius-vdom-override {disable | enable}
    set remote-auth {enable | disable}
    set remote-group <name>
    set schedule <schedule-name>
    set ssh-public-key1 "<key-type> <key-value>"
    set ssh-public-key2 "<key-type> <key-value>"
    set ssh-public-key3 "<key-type> <key-value>"
    set trusthost1 <address_ipv4mask>
    set trusthost2 <address_ipv4mask>
    set trusthost3 <address_ipv4mask>
    set vdom <vdom_name>
    set wildcard {enable | disable}
    config dashboard
      edit alert
      edit app-usage
      edit dlp-usage
      edit jsconsole
      edit licinfo
      edit pol-usage
      edit sessions
      edit statistics
      edit sysinfo
      edit sysop
      edit sysres
      edit top-attacks
      edit top-viruses
      edit tr-history
        set column <column_number>
        set status {close | open}
        set <custom_options>
      end
    end
  end
```

Variable	Description	Default
`accprofile <profile-name>`	Enter the name of the access profile to assign to this administrator account. Access profiles control administrator access to FortiGate features.	No default.
`comments <comments_string>`	Enter the last name, first name, email address, phone number, mobile phone number, and pager number for this administrator. Separate each attribute with a comma, and enclose the string in double-quotes. The total length of the string can be up to 128 characters. (Optional)	null
`force-password-change {enable | disable}`	Enable to require this administrator to change password at next login. Disabling this option does not prevent required password change due to password policy violation or expiry.	`disable`

Variable	Description	Default
ip6-trusthost1 <address_ipv6mask>	Any IPv6 address and netmask from which the administrator can connect to the FortiGate unit. If you want the administrator to be able to access the FortiGate unit from any address, set the trusted hosts to ::/0.	::/0
ip6-trusthost2 <address_ipv6mask>	Any IPv6 address and netmask from which the administrator can connect to the FortiGate unit. If you want the administrator to be able to access the FortiGate unit from any address, set the trusted hosts to ::/0.	::/0
ip6-trusthost3 <address_ipv6mask>	Any IPv6 address and netmask from which the administrator can connect to the FortiGate unit. If you want the administrator to be able to access the FortiGate unit from any address, set the trusted hosts to ::/0.	::/0
password <admin_password>	Enter the password for this administrator.	null
password-expire YYYY-MM-DD HH:MM:SS	Enter the date and time that this administrator's password expires. Enter zero values for no expiry.	0000-00-00 00:00:00
peer-auth {disable | enable}	Set to enable peer certificate authentication (for HTTPS admin access).	disable
peer-group <peer-grp>	Name of peer group defined under config user peergrp or user group defined under config user group. Used for peer certificate authentication (for HTTPS admin access).	null
radius-accprofile-override {disable | enable}	Enable RADIUS authentication override for the access profile of the administrator.	disable
radius-vdom-override {disable | enable}	Enable RADIUS authentication override for the (wildcard only) administrator.	disable
remote-auth {enable | disable}	Enable or disable authentication of this administrator using a remote RADIUS, LDAP, or TACACS+ server.	disable
remote-group <name>	Enter the administrator user group name, if you are using RADIUS, LDAP, or TACACS+ authentication. This is only available when remote-auth is enabled.	No default.
schedule <schedule-name>	Restrict times that an administrator can log in. Defined in config firewall schedule. Null indicates that the administrator can log in at any time.	null
ssh-public-key1 "<key-type> <key-value>"	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application. <key type> is ssh-dss for a DSA key or ssh-rsa for an RSA key. <key-value> is the public key string of the SSH client.	No default.
ssh-public-key2 "<key-type> <key-value>"		No default.
ssh-public-key3 "<key-type> <key-value>"		No default.
trusthost1 <address_ipv4mask>	Any IP address or subnet address and netmask from which the administrator can connect to the FortiGate unit. If you want the administrator to be able to access the FortiGate unit from any address, set the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0.	0.0.0.0 0.0.0.0
trusthost2 <address_ipv4mask>	Any IP address or subnet address and netmask from which the administrator can connect to the FortiGate unit. If you want the administrator to be able to access the FortiGate unit from any address, set the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0.	0.0.0.0 0.0.0.0

Variable	Description	Default
`trusthost3 <address_ipv4mask>`	Any IP address or subnet address and netmask from which the administrator can connect to the FortiGate unit. If you want the administrator to be able to access the FortiGate unit from any address, set the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0.	`127.0.0.1 255.255.255.255`
`vdom <vdom_name>`	Enter the name of the VDOM this account belongs to. (Optional)	No default.
`wildcard {enable | disable}`	Enable `wildcard` to allow all accounts on the RADIUS server to log on to the FortiGate unit as administrator. Disable `wildcard` if you want to allow only the specified administrator to log on. This is available when `remote-auth` is enabled.	`disable`
`dashboard`	Customize the system dashboard and usage widgets for this administrator.	
`<module_name>`	Name of the system dashboard or usage widget to configure: `alert` — Alert message console dashboard widget `app-usage` — Top application usage widget `dlp-usage` — DLP archive usage widget `jsconsole` — CLI console dashboard widget `licinfo` — License information dashboard widget `pol-usage` — Top Policy usage widget `sessions` — Top sessions dashboard widget `statistics` — Log and archive statistics dashboard widget `sysinfo` — System information dashboard widget `sysop` — Unit operation dashboard widget `sysres` — System resources dashboard widget `top-attacks` —Top attacks dashboard widget `top-viruses` —Top viruses dashboard widget `tr-history` —Traffic history dashboard widget	
`column <column_number>`	Column in which the dashboard module appears. Values `1` or `2`. Available for all dashboard modules.	0
`status {close | open}`	Set whether the widget is open or closed on the dashboard.	
`<custom_options>`	The custom options for the usage and dashboard widgets are listed below.	
Dashboard and usage widget variables		
`alert`	Configure the information displayed on the alert message console by enabling or disabling the following options: **`show-admin-auth`** — admin authentication failures **`show-amc-bypass`** — AMC interface bypasses **`show-conserve-mode`** — conserve mode alerts **`show-device-update`** — device updates **`show-disk-failure`** — disk failure alerts **`show-fds-quota`** — FortiGuard Distribution System alerts **`show-fds-update`** — FortiGuard Distribution System updates **`show-firmware-change`** — firmware upgrades and downgrades **`show-power-supply`** — power supply alerts **`show-system-restart`** — system restart alerts	

Variable	Description	Default
app-usage	Configure the operation of the top application usage widget: **display-format {chart | table}**— display data in a chart or a table. **refresh-interval <interval_int>** — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable **report-by {destination | source}**— display application usage according to the source address or destination address of the sessions. **reslove-host {disable | enable}**— display host names (instead of IP addresses). **show-auth-use {disable | enable}**— include the user name of authenticated users. **sort-by {bytes | msg-counts}**— sort information by the amount of data (bytes) or the number of session (msg-counts). **top-n <results_int>** — set the number of results to display. The default value displays the top 10 results. **vdom <vdom_str>** — display results for a specific VDOM.	
dlp-usage	For the DLP archive usage widget set the column and open and closed status and set the following options: **dlp-protocols {protocols}**— enter the names of the protocols to display information for. **refresh-interval <interval_int>** — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. **report-by {dlp-rule | policy | profile | protocol}**— organize the information displayed by DLP rule name, firewall policy ID, protection profile name, or DLP protocol. **sort-by {bytes | msg-counts}**— sort information by the amount of data (bytes) or the number of session (msg-counts). **top-n <results_int>** — set the number of results to display. The default value displays the top 10 results. **vdom <vdom_str>** — display results for a specific VDOM.	
jsconsole	Set the dashboard column and open and closed status of the CLI console widget.	
licinfo	Set the dashboard column and open and closed status of the License information widget.	
pol-usage	For the top policy usage widget set the column and open and closed status and set the following options: **display-format {chart | table}**— display data in a chart or a table. **refresh-interval <interval_int>** — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. **sort-by {bytes | msg-counts}**— sort information by the amount of data (bytes) or the number of session (msg-counts). **top-n <results_int>** — set the number of results to display. The default value displays the top 10 results. **vdom <vdom_str>** — display results for a specific VDOM.	

Variable	Description	Default
sessions	For the top session dashboard widget set the dashboard column and open and closed status and set the following options: **display-format {chart | table}**— display data in a chart or a table. **refresh-interval <interval_int>** — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. **sort-by {bytes | msg-counts}**— sort information by the amount of data (bytes) or the number of session (msg-counts). **top-n <results_int>** — set the number of results to display. The default value displays the top 10 results. **vdom <vdom_str>** — display results for a specific VDOM.	
statistics	Set the dashboard column and open and closed status of the log and archive statistics dashboard widget.	
sysinfo	Set the dashboard column and open and closed status of the system information dashboard widget.	
sysop	Set the dashboard column and open and closed status of the unit operation dashboard widget.	
sysres	For the system resources dashboard widget set the dashboard column and open and closed status and set the following options: **show-fds-chart {disable | enable}**— display the FortiGuard log disk usage chart **show-fortianalyzer-chart {disable | enable}**— display the FortiAnalyzer disk usage chart	
top-attacks	For the top attacks dashboard widget set the dashboard column and open and closed status and set the following options: **refresh-interval <interval_int>** — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. **top-n <results_int>** — set the number of results to display. The default value displays the top 10 results.	
top-viruses	For the top viruses dashboard widget set the dashboard column and open and closed status and set the following options: **refresh-interval <interval_int>** — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. **top-n <results_int>** — set the number of results to display. The default value displays the top 10 results.	
tr-history	For the traffic history dashboard widget set the dashboard column and open and closed status and set the following options: **refresh {disable | enable}**— enable automatically refreshing the display **interface <interface_name>** — name of interface monitored for traffic history data.	

Example

Use the following commands to add a new administrator account named new_admin with the password set to p8ssw0rd and that includes an access profile named policy_profile. It is accessible on the main_office VDOM. Administrators that log in to this account will have administrator access to the FortiGate unit from any IP address. The dashboard setting alert > show-system-restart is enabled and displays in column 2 of the FortiOS GUI.

```
config system admin
  edit new_admin
    set password p8ssw0rd
    set accprofile policy_profile
    set vdom main_office
    config dashboard
      edit alert
        set column 2
        set status open
        show-system-restart enable
      end
  end
end
```

History

FortiOS v2.80	Revised.
FortiOS v3.0	Added `email-address`, `first-name`, `last-name`, `mobile-number`, `pager-number`, `phone-number`, `radius-auth`, `radius-group`, `wildcard` fields.
FortiOS v3.0 MR1	Added `is-admin and vdom` fields.
FortiOS v3.0 MR3	Removed is-admin. Combined `first-name`, `last-name`, `email-address`, `phone-number`, `mobile-number`, `pager-number` and put in field `comments` (concatenated).
FortiOS v3.0 MR4	Added dashboard configuration fields/variables, `password`.
FortiOS v3.0 MR5	Added description of `password` setup.
FortiOS v3.0 MR6	Added `schedule`. Included description of `ReadOnlyAdmin`. Added `config dashboard` subcommand. Renamed field `radius-auth` to `remote-auth`. Renamed field `radius-group` to `remote-group`.
FortiOS v3.0 MR7	Added `radius-vdom-override` and `radius-accprofile-override`.
FortiOS v4.0 MR1	Added `force-password-change`, `ip6-trusthost1`, `ip6-trusthost2`, `ip6-trusthost3`, and `password-expire`. Removed `moduleid`.

Related topics

- system accprofile

alertemail

Use this command to configure the FortiGate unit to access an SMTP server to send alert emails. This command is global in scope.

To configure alertemail settings you must first configure the server, and enable authenticate. Then you will be able to see all the fields.

Note: You must configure the server setting under `config system alertemail` before the commands under `config alertemail` become accessible. If vdoms are enabled, `config system alertemail` is a global command, and `config alertemail` is per vdom. For more information on `config alertemail`, see "alertemail" on page 67.

Syntax

```
config system alertemail
  set authenticate {disable | enable}
  set password <password_str>
  set port <port_integer>
  set server {<name-str> | <address_ipv4>}
  set username <username_str>
end
```

Variable	Description	Default
`authenticate {disable | enable}`	Enable SMTP authentication if the FortiGate unit is required to authenticate before using the SMTP server. This variable is accessible only if `server` is defined.	`disable`
`password <password_str>`	Enter the password that the FortiGate unit needs to access the SMTP server. This variable is accessible only if `authenticate` is enabled and `server` is defined.	No default.
`port <port_integer>`	Change the TCP port number that the FortiGate unit uses to connect to the SMTP server. The standard SMTP port is 25. You can change the port number if the SMTP server has been configured to use a different port.	25
`server {<name-str> | <address_ipv4>}`	Enter the name of the SMTP server, in the format `smtp.domain.com`, to which the FortiGate unit should send email. Alternately, the IP address of the SMTP server can be entered. The SMTP server can be located on any network connected to the FortiGate unit.	No default.
`username <username_str>`	Enter the user name for the SMTP server that the FortiGate unit uses to send alert emails. This variable is accessible only if `authenticate` is enabled and `server` is defined.	No default.

Examples

This example shows how to configure the FortiGate unit to send alert emails using the SMTP server `smtp.example.com`. The order of the fields is important. The server must be defined first. Then authentication needs to be next. The FortiGate unit uses the user name `admin2` and the password `h8rdt0g3uss` to connect to the SMTP server.

```
config system alertemail
  set server smtp.example.com
  set authenticate enable
  set password h8rdt0g3uss
```

```
    set username admin2
  end
```

History

FortiOS v3.0	Command created from `alertemail` command.
FortiOS v3.0 MR7	Added the `port` field.

amc

Use this command to configure AMC ports on your FortiGate unit. The number of AMC ports on your FortiGate unit will vary by model.

When you first get your FortiGate unit with AMC ports, the AMC ports must be configured before the ports can be used. The settings are different for single width and double width ports.

The auto setting will recognize any card used in the AMC port, but when you remove the card it will not retain any configuration settings.

The `asm-cx4, asm-disk`, `asm-fb4`, `asm-cx4, adm-xb2`, and `adm-fb8` settings will retain any configurations related to that card until a different type of card is inserted. For example if the port is set to `asm-disk` with configurations for that disk, and if the disk needs to be replaced it can be removed and it or one of the same type can be re-inserted with the FortiGate unit retaining all the related configurations.

To use an AMC slot that is configured for one type of card with a different type of card, you must first set the slot to none, and then reconfigure the slot for the new type of card. This will remove all configuration that was associated with the previous AMC card.

Syntax

```
config system amc
  set {sw1 | sw2} {asm-cx4 | asm-disk | asm-fb4 | asm-fx2 | auto | none}
  set {dw1 | dw2} {adm-fb8 | adm-xb2 | auto | none}
end
```

Variable	Description	Default
`{sw1 | sw2} {asm-cx4 | asm-disk | asm-fb4 | asm-fx2 | auto | none}`	Configure this single width AMC port for the following type of card. **`asm-cx4`** — AMC single width, 4G bypass **`asm-disk`** — AMC Single width SCSI hard disk card, such as ASM-S08 **`asm-fb4`** — AMC single width 4G NP2 network interface card **`asm-fx2`** — AMC single width, 2G bypass **`auto`** — support any single width card **`none`** — not configured, disable slot	`none`
`{dw1 | dw2} {adm-fb8 | adm-xb2 | auto | none}`	Configure this double width AMC port for the following type of card. **`adm-fb8`** — AMC double width 8G NP2 network interface card **`adm-xb2`** — AMC double width 2XG NP2 card **`auto`** — support any card that is inserted **`none`** — not configured, disable slot	`none`

History

FortiOS v3.0 MR7 New command.

FortiOS v4.0 Added `asm-cx4` and `asm-fx2` to list of supported AMC single width cards.

arp-table

Use this command to manually configure add ARP table entries to the FortiGate unit. ARP table entries consist of a interface name, an IP address, and a MAC address.

Limits for the number of ARP table entries are software limits set by the FortiGate configuration as documented in the *FortiGate Maximum Values Matrix* document.

This command is available per VDOMs.

Syntax

```
config system arp-table
  edit <table_value>
    set interface <port>
    set ip <address_ipv4>
    set mac <mac_address>
  end
```

Variable	Description	Default
`interface <port>`	Enter the interface this ARP entry is associated with	No `default`
`ip <address_ipv4>`	Enter the IP address of the ARP entry.	No default.
`mac <mac_address>`	Enter the MAC address of the device entered in the table, in the form of xx:xx:xx:xx:xx:xx.	No default.

Examples

This example adds an entry to the arp table with a MAC address of 00-09-0f-69-00-7c and an IP address of 172.20.120.161 on the port2 interface.

```
config system arp-table
  edit 3
    set interface port2
    set ip 172.20.120.161
    set mac 00:09:0f:69:00:7c
  end
```

History

FortiOS v3.0 MR2 New command.

Related topics

- get system arp

auto-install

Use this command to configure automatic installation of firmware and system configuration from a USB disk when the FortiGate unit restarts. This command is available only on units that have a USB disk connection.

If you set both configuration and firmware image update, both occur on the same reboot. The FortiGate unit will not reload a firmware or configuration file that is already loaded.

Third-party USB disks are supported; however, the USB disk must be formatted as a FAT16 drive. No other partition type is supported.

To format your USB Disk when its connected to your FortiGate unit, at the CLI prompt type "`exe usb-disk format`".

To format your USB disk when it is connected to a Windows system, at the command prompt type "`format <drive_letter>: /FS:FAT /V:<drive_label>`" where `<drive_letter>` is the letter of the connected USB drive you want to format, and `<drive_label>` is the name you want to give the USB disk volume for identification.

Note: This command is available only when a USB key is installed on the FortiGate unit. Formatting your USB disk will delete all information on your USB disk.

Syntax

```
config system auto-install
  set auto-install-config {disable | enable}
  set auto-install-image {disable | enable}
  set default-config-file
  set default-image-file
end
```

Variable	Description	Default
`auto-install-config {disable | enable}`	Enable or disable automatic loading of the system configuration from a USB disk on the next reboot.	`disable`
`auto-install-image {disable | enable}`	Enable or disable automatic installation of firmware from a USB disk on the next reboot.	`disable`
`default-config-file`	Enter the name of the configuration file on the USB disk.	`fgt_system.conf`
`default-image-file`	Enter the name of the image file on the USB disk.	`image.out`

History

FortiOS v3.0 New.

autoupdate clientoverride

Use this command to receive updates on a different interface than the interface connected to the FortiGuard Distribution Network (FDN). This command changes the source IP address of update requests to the FortiGuard server, causing it to send the update to the modified source address.

This is useful if your company uses an internal updates server instead of FDN.

Syntax

```
config system autoupdate clientoverride
  set status {enable | disable}
  set address <address_ipv4>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable or disable the ability to override the FDN interface address.	`disable`
`address <address_ipv4>`	Enter the IP address or fully qualified domain name to receive updates from.	No default.

Example

This example shows how to add a push update client IP address 192.168.21.145 which is on the port 4 interface.

```
config system autoupdate clientoverride
  set address 192.168.21.145
  set status enable
end
```

History

FortiOS v2.80 MR6 Added.

Related topics

- system autoupdate override
- system autoupdate push-update
- system autoupdate schedule
- system autoupdate tunneling
- execute update-ase

autoupdate override

Use this command to specify an override FDS server.

If you cannot connect to the FortiGuard Distribution Network (FDN) or if your organization provides updates using their own FortiGuard server, you can specify an override FDS server so that the FortiGate unit connects to this server instead of the FDN.

Note: If you are unable to connect to the FDS server, even after specifying an override server, it is possible your ISP is blocking the lower TCP and UDP ports for security reasons. Contact your ISP to make sure they unblock TCP and UDP ports 1025 to 1035 to enable FDS server traffic. Another option is to use config global set `ip-src-port-range` to move the ports used to a higher range and avoid any possible problems. For more information, see "global" on page 423.

Syntax

```
config system autoupdate override
  set status {enable | disable}
  set address <FDS_address>
  set failover {enable | disable}
end
```

Variable	Description	Default
`status {enable | disable}`	Enable or disable overriding the default FDS server.	`disable`
`address <FDS_address>`	Enter the IP address or fully qualified domain name of the override FDS server.	No default.
`failover {enable | disable}`	Enable or disable FDS server failover. If you enable failover, if the FortiGate unit cannot reach the override FDS server it will failover to the public FDS servers.	`enable`

Example

This example shows how to add and enable your company's own FDS override server with an IP address of 192.168.87.145.

```
config system autoupdate override
  set address 192.168.87.145
  set status enable
end
```

History

FortiOS v2.80 Revised.

Related topics

- system autoupdate push-update
- system autoupdate schedule
- system autoupdate tunneling
- execute update-ase
- execute update-ips

autoupdate push-update

Use this command to configure push updates. The FortiGuard Distribution Network (FDN) can push updates to FortiGate units to provide the fastest possible response to critical situations such as software exploits or viruses. You must register the FortiGate unit before it can receive push updates.

When you configure a FortiGate unit to allow push updates, the FortiGate unit sends a SETUP message to the FDN. The next time an update is released, the FDN notifies all FortiGate units that are configured for push updates that a new update is available. Within 60 seconds of receiving a push notification, the FortiGate unit requests an update from the FDN.

By using this command, you can enable or disable push updates. You can also configure push IP address and port overrides. If the FDN must connect to the FortiGate unit through a NAT device, you must configure port forwarding on the NAT device and add the port forwarding information to the push update override configuration.

Note: You cannot receive push updates through a NAT device if the external IP address of the NAT device is dynamic (for example, set using PPPoE or DHCP).

Syntax

```
config system autoupdate push-update
  set system status {enable | disable}
  set system override {enable | disable}
  set system address <push_ipv4>
  set system port <FDN_port>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable or disable FDN push updates.	`disable`
`override {enable | disable}`	Enable an override of push updates. Select enable if the FortiGate unit connects to the FDN through a NAT device.	`disable`
`address <push_ipv4>`	Enter the External IP address that the FDN connects to if you want to enable push override. This is the address of the external interface of your NAT device.	`0.0.0.0`
`port <FDN_port>`	Enter the port that the FDN connects to. This can be port 9443 by default or a different port that you assign.	`9443`

Example

This example shows how to enable push updates on port 9993.

```
config system autoupdate push-update
  set status enable
  set port 9993
end
```

History

FortiOS v2.80 Revised.

Related topics

- system autoupdate override, system autoupdate schedule, system autoupdate tunneling
- execute update-ase, execute update-ips

autoupdate schedule

Use this command to enable or disable scheduled FDN updates at regular intervals throughout the day, once a day, or once a week.

To have your FortiGate unit to update at a random time during a particular hour, select a time that includes 60 minutes as this will choose a random time during that hour for the scheduled update.

Syntax

```
config system autoupdate schedule
  setsystem status {enable | disable}
  setsystem frequency {every | daily | weekly}
  setsystem time <hh:mm>
  setsystem day <day_of_week>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable or disable scheduled updates.	`disable`
`frequency {every | daily | weekly}`	Schedule the FortiGate unit to check for updates every hour, once a day, or once a week. Set `interval` to one of the following: **`every`** — Check for updates periodically. Set `time` to the time interval to wait between updates. **`daily`** — Check for updates once a day. Set `time` to the time of day to check for updates. **`weekly`** — Check for updates once a week. Set `day` to the day of the week to check for updates. Set `time` to the time of day to check for updates.	`every`
`time <hh:mm>`	Enter the time at which to check for updates. **`hh`** — 00 to 23 **`mm`** — 00-59, or 60 for random minute	`00:00`
`day <day_of_week>`	Enter the day of the week on which to check for updates. Enter one of: `Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, or `Saturday`. This option is available only when `frequency` is set to `weekly`.	`Monday`

Example

This example shows how to configure the FortiGate unit to check the FortiGuard Distribution Network (FDN) for updates once a day at 3:00 in the morning.

```
config system autoupdate schedule
  set frequency daily
  set time 03:00
  set status enable
end
```

This example is the same as the above example but it will check for updates once a day at sometime between 3:00 and 4:00 in the morning.

```
config system autoupdate schedule
  set frequency daily
  set time 03:60
  set status enable
end
```

History

FortiOS v2.80	Revised.
FortiOS v2.80 MR2	Can set `time` as well as `day` for weekly updates.

Related topics

- system autoupdate override
- system autoupdate push-update
- system autoupdate tunneling
- system global

autoupdate tunneling

Use this command to configure the FortiGate unit to use a proxy server to connect to the FortiGuard Distribution Network (FDN). You must enable tunneling so that you can use the proxy server, and also add the IP address and port required to connect to the proxy server. If the proxy server requires authentication, add the user name and password required to connect to the proxy server.

The FortiGate unit connects to the proxy server using the HTTP CONNECT method, as described in RFC 2616. The FortiGate unit sends a HTTP CONNECT request to the proxy server (optionally with authentication information) specifying the IP address and port required to connect to the FDN. The proxy server establishes the connection to the FDN and passes information between the FortiGate unit and the FDN.

The CONNECT method is used mostly for tunneling SSL traffic. Some proxy servers do not allow CONNECT to connect to any port; proxy servers restrict the allowed ports to the well known ports for HTTPS and perhaps some other similar services. FortiGate autoupdates use HTTPS on port 8890 to connect to the FDN, so your proxy server may need to be configured to allow connections on this port.

Syntax

```
config system autoupdate tunneling
  set address <proxy_address>
  set password <password>
  set port <proxy_port>
  set status {enable | disable}
  set username <name>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable or disable tunneling.	`disable`
`address <proxy_address>`	The IP address or fully qualified domain name of the proxy server.	No default.
`port <proxy_port>`	The port required to connect to the proxy server.	`0`
`username <name>`	The user name used to connect to the proxy server.	No default.
`password <password>`	The password to connect to the proxy server if one is required.	No default.

Example

This example shows how to enable tunneling where the FortiGate unit must connect to a proxy server with IP address 192.168.50.134 that uses port 8080, requires the user id `proxy_user` and the password `proxy_pwd`.

```
config system autoupdate tunneling
  set address 192.168.50.134
  set port 8080
  set username proxy_user
  set password proxy_pwd
  set status enable
end
```

History

FortiOS v2.80 Revised.

Related topics

- system autoupdate override
- system autoupdate push-update
- system autoupdate schedule

aux

Use this command to configure the AUX port. You can use a modem connected to the AUX port to remotely connect to a console session on the FortiGate unit. The AUX port is located near the console port, but not all FortiGate models have an AUX port.

The main difference between the standard console port and the AUX port is that the standard console port is for local serial console connections only. An AUX port cannot accept a modem connection to establish a remote console connection. The AUX console port allows you to establish a local connection, but it has some limitations the standard console port does not have.

- The AUX port will not display the booting messages that the standard console connection displays.
- The AUX port will send out modem initializing strings (AT strings) that will appear on an AUX console session at the start.

Syntax

```
config system aux
  set baudrate <baudrate>
end
```

<baudrate> is the speed of the connection. It can be set to one of the following: 9600, 19200, 38400, 57600, or 115200. The default is 9600.

Ensure devices on both ends of the connection are set to the same baudrate.

History

FortiOS v3.0 MR1 New.

Related topics

- system console

bug-report

Use this command to configure a custom email relay for sending problem reports to Fortinet customer support.

Syntax

```
config system bug-report
  set auth {no | yes}
  set mailto <email_address>
  set password <password>
  set server <servername>
  set username <name>
  set username-smtp <account_name>
end
```

Variable	Description	Default
`auth {no | yes}`	Enter `yes` if the SMTP server requires authentication or `no` if it does not.	`no`
`mailto <email_address>`	The email address for bug reports. The default is `bug_report@fortinetvirussubmit.com`.	See description.
`password <password>`	If the SMTP server requires authentication, enter the password required.	No default.
`server <servername>`	The SMTP server to use for sending bug report email. The default server is `fortinetvirussubmit.com`	See description.
`username <name>`	A valid user name on the specified SMTP server. The default user name is `bug_report`.	See description.
`username-smtp <account_name>`	A valid user name on the specified SMTP server. The default user name is `bug_report`.	See description.

Example

This example shows how to configure the FortiGate unit to send bug report email from the ourmailserver.com email server to bug_report@ourcompany.com using the User1 account. The email server requires authentication.

```
config system bug-report
  set auth yes
  set mailto bug_report@ourcompany.com
  set password 123456
  set server ourmailserver.com
  set username OurAdmin
end
```

History

FortiOS v2.80	New.
FortiOS v2.80 MR2	Command changed from `config bug-report` to `config system bug-report`.
FortiOS v3.0	Changed `username_smtp` to `username-smtp`.
FortiOS v3.0 MR1	Added `mailto` field.

Related topics

- system dns

central-management

Use this command to configure a central management server for this FortiGate unit. Central management uses a remote server to backup, restore configuration, and monitor the FortiGate unit. The remote server can be either a FortiManager or a FortiGuard server.

This command replaces the `config system fortimanager` command from earlier versions.

Syntax

```
config system central-management
  set allow-monitor {enable | disable}
  set allow-push-configuration {enable | disable}
  set allow-pushd-firmware {enable | disable}
  set allow-remote-firmware-upgrade {enable | disable}
  set authorized-manager-only {enable | disable}
  set auto-backup {enable | disable}
  set fmg <fmg_ipv4>
  set schedule-config-restore {enable | disable}
  set schedule-script-restore {enable | disable}
  set serial-number <fmg_serial_number>
  set status {enable | disable}
  set type { fortiguard | fortimanager }
  set vdom <name_string>
end
```

Variable	Description	Default
`allow-monitor {enable | disable}`	Select to allow the remote service to monitor your FortiGate unit.	`disable`
`allow-push-configuration {enable | disable}`	Select to enable firmware image push updates for your FortiGate unit.	`disable`
`allow-pushd-firmware {enable | disable}`	Select to enable push firmware.	`disable`
`allow-remote-firmware-upgrade {enable | disable}`	Select to allow the remote service to upgrade your FortiGate unit with a new firmware image.	`disable`
`authorized-manager-only {enable | disable}`	Select to restrict access to the authorized manger only.	`disable`
`auto-backup {enable | disable}`	Select to enable automatic uploading of your FortiGate configuration to the remote service. This creates a back up of your current configuration every time you log out of your FortiGate unit and uploads the backed up configuration file to the remote service.	`disable`
`fmg <fmg_ipv4>`	Enter the IP address or FQDN of the remote FortiManager server.	`null`
`schedule-config-restore {enable | disable}`	Select to enable scheduling the restoration of your FortiGate unit's configuration.	`disable`
`schedule-script-restore {enable | disable}`	Select to enable the restoration of your FortiGate unit's configuration through scripts.	`disable`
`serial-number <fmg_serial_number>`	Enter the serial number of the remote FortiManager server.	`null`
`status {enable | disable}`	Select to enable remote management service for your FortiGate unit.	`disable`

Variable	Description	Default
`type { fortiguard | fortimanager }`	Select the type of management server as one of - `fortiguard` or `fortimanager`. You can enable remote management from a FortiManager unit or the FortiGuard Analysis and Management Service.	`fortimanager`
`vdom <name_string>`	Enter the name of the vdom to use when communicating with the FortiManager unit. This field is optional.	`root`

Example

This example shows how to configure remote service between a FortiGate unit and a FortiManager unit that has an IP address of 172.16.55.121 and a serial number of `FMG40A3906500505`. The connection between the FortiGate and FortiManager units is over vdom_1 VDOM.

```
config system central-management
  set status enable
  set type fortimanager
  set fmg 172.16.55.121
  set serial-number FMG40A3906500505
  set auto-backup enable
  set vdom vdom_1
end
```

History

FortiOS v4.0 New. Replaces the older `config system fortimanager` command.

Related topics

- system dns

console

Use this command to set the console command mode, the number of lines displayed by the console, and the baud rate.

Fortigate-1000A, 1000AFA2, and 3000A models have an AUX port that can be used for remote console connections using a modem. This port on these models is configured with the system aux command, see "aux" on page 404.

Note: If this FortiGate unit is connected to a FortiManager unit running scripts, `output` must be set to `standard` for scripts to execute properly.

If this FortiGate unit is connected to a FortiManager unit running scripts, `output` must be set to `standard` for scripts to execute properly.

Syntax

```
config system console
  set baudrate <speed>
  set mode {batch | line}
  set output {standard | more}
end
```

Variable	Description	Default
`baudrate <speed>`	Set the console port baudrate. Select one of 9600, 19200, 38400, 57600, or 115200.	`9600`
`mode {batch | line}`	Set the console mode to line or batch. Used for autotesting only.	`line`
`output {standard | more}`	Set console output to standard (no pause) or more (pause after each screen is full, resume on keypress). This setting applies to `show` or `get` commands only.	more

Example

This example shows how to set the baudrate to 38400 and set the output style to more so it will pause after each screen full of information.

```
config system console
  set baudrate 38400
  set output more
end
```

History

FortiOS v2.80 Revised.

FortiOS v2.80 MR2 Command changed from `config console` to `config system console`.

FortiOS v2.80 MR4 `page` field removed. `output` field added.

Related topics

- system aux

dhcp reserved-address

Use this command to reserve an IP address for a particular client identified by its device MAC address and type of connection. The DHCP server then always assigns the reserved IP address to the client. You can define up to 200 reserved addresses.

Note: For this configuration to take effect, you must configure at least one DHCP server using the `config system dhcp server` command, see "dhcp server" on page 410.

Syntax

```
config system dhcp reserved-address
  edit <name_str>
    set ip <address_ipv4>
    set mac <address_hex>
    set type {regular | ipsec}
  end
```

Variable	Description	Default
`ip <address_ipv4>`	Enter the IP address.	0.0.0.0
`mac <address_hex>`	Enter the MAC address.	00:00:00:00:00:00
`type {regular | ipsec}`	Enter the type of the connection to be reserved: **`regular`** — Client connecting through regular Ethernet **`IPSec`** — Client connecting through IPSec VPN	`regular`

Example

Use the following command to add a reserved address named `client_1` consisting of IP address 192.168.110.3 and MAC address 00:09:0F:0A:01:BC for a regular ethernet connection.

```
config system dhcp reserved-address
  edit client_1
    set ip 192.168.110.3
    set mac 00:09:0F:0A:01:BC
    set type regular
  end
```

History

FortiOS v2.80 Substantially revised.

FortiOS v3.0 MR7 Maximum number of reserved addresses increased to 200 for all models.

Related topics

- system dhcp server
- system interface

dhcp server

Use this command to add one or more DHCP servers for any FortiGate interface. As a DHCP server, the interface dynamically assigns IP addresses to hosts on a network connected to the interface.

You can use the `config system dhcp reserved` command to reserve an address for a specific MAC address. For more information see "system dhcp reserved-address" on page 409.

You can add more than one DHCP server to a single interface to be able to provide DHCP services to multiple networks. For more information on configuring your network and FortiGate unit to use multiple DHCP servers on one interface, see the ***System DHCP*** chapter in the ***Administration Guide*** for your FortiGate unit.

This command is available in NAT/Route mode only.

Syntax

```
config system dhcp server
  edit <dhcpservername>
    set conflicted-ip-timeout <timeout_int>
    set default-gateway <address_ipv4>
    set dns-server1 <address_ipv4>
    set dns-server2 <address_ipv4>
    set dns-server3 <address_ipv4>
    set domain <domain_name_str>
    set enable {enable | disable}
    set end-ip <address_ipv4>
    set interface <interface_name>
    set ipsec-lease-hold <release_seconds>
    set lease-time <seconds>
    set netmask <mask>
    set option1 <option_code> [<option_hex>]
    set option2 <option_code> [<option_hex>]
    set option3 <option_code> [<option_hex>]
    set server-type <type>
    set start-ip <address_ipv4>
    set wins-server1 <wins_ipv4>
    set wins-server2 <wins_ipv4>
    config exclude-range
    edit <excl_range_num>
    set end-ip <excl_ipv4>
    set start-ip <excl_ipv4>
    end
  end
```

Variable	Description	Default
`conflicted-ip-timeout <timeout_int>`	Enter the time in seconds to wait before a conflicted IP address is removed from the DHCP range. Valid range is from 60 to 8640000 seconds (1 minute to 100 days).	1800
`default-gateway <address_ipv4>`	The IP address of the default gateway that the DHCP server assigns to DHCP clients.	0.0.0.0
`dns-server1 <address_ipv4>`	The IP address of the first DNS server that the DHCP server assigns to DHCP clients.	0.0.0.0
`dns-server2 <address_ipv4>`	The IP address of the second DNS server that the DHCP server assigns to DHCP clients.	0.0.0.0

Variable	Description	Default
dns-server3 <address_ipv4>	The IP address of the third DNS server that the DHCP server assigns to DHCP clients.	0.0.0.0
domain <domain_name_str>	Domain name suffix for the IP addresses that the DHCP server assigns to DHCP clients.	No default.
enable {enable | disable}	Enable or disable this DHCP server.	enable
end-ip <address_ipv4>	The ending IP for the range of IP addresses that this DHCP server assigns to DHCP clients. The IP range is defined by the start-ip and the end-ip field which should both be in the same subnet.	0.0.0.0
interface <interface_name>	The interface of the DHCP server.	internal
ipsec-lease-hold <release_seconds>	Set the DHCP lease release delay in seconds for DHCP-over-IPSec tunnels when the tunnel goes down. A value of 0 disables the forced expiry of the DHCP-over-IPSec leases. Visible only when server-type is set to ipsec.	60
lease-time <seconds>	The interval in seconds after which a DHCP client must ask the DHCP server for new settings. The lease duration must be between 300 and 864,000 seconds (10 days). Set lease-time to 0 for an unlimited lease time.	604,800 (7 days)
netmask <mask>	The DHCP client netmask assigned by the DHCP server.	0.0.0.0
option1 <option_code> [<option_hex>] option2 <option_code> [<option_hex>] option3 <option_code> [<option_hex>]	The first, second, and third custom DHCP options that can be sent by the DHCP server. option_code is the DHCP option code in the range 1 to 255. option_hex is an even number of hexadecimal characters. For detailed information about DHCP options, see RFC 2132, DHCP Options and BOOTP Vendor Extensions.	No default.
server-type <type>	Enter the type of client to serve: **regular** — Client connects through regular Ethernet **IPSec** — Client connects through IPSec VPN	regular
start-ip <address_ipv4>	The starting IP for the range of IP addresses that this DHCP server assigns to DHCP clients. The IP range is defined by the start-ip and the end-ip fields which should both be in the same subnet.	0.0.0.0
wins-server1 <wins_ipv4>	The IP address of the first WINS server that the DHCP server assigns to DHCP clients.	0.0.0.0
wins-server2 <wins_ipv4>	The IP address of the second WINS server that the DHCP server assigns to DHCP clients.	0.0.0.0
config exclude-range	Configure a range of IP addresses to exclude from the list of DHCP addresses that are available.	
edit <excl_range_num>	Enter an integer ID for this exclusion range. You can add up to 16 exclusion ranges of IP addresses that the FortiGate DHCP server cannot assign to DHCP clients	None
start-ip <excl_ipv4>	The start IP address in the exclusion range. The start IP and end IP must be in the same subnet. This field applies to exclude-range.	0.0.0.0
end-ip <excl_ipv4>	The end IP address in the exclusion range. The start IP and end IP must be in the same subnet. This field applies to exclude-range.	0.0.0.0

Example

Use the following command to add a DHCP server named new_dhcp. This DHCP server assigns IP addresses to computers connected to the same network as the internal interface. The IP addresses assigned are in the range 192.168.33.100 to 192.168.33.200. The example DHCP configuration also sets the netmask, default gateway, two DNS server IP addresses, the lease time, and one WINS server.

```
config system dhcp server
  edit new_dhcp
    set interface internal
    set start-ip 192.168.33.100
    set end-ip 192.168.33.200
    set netmask 255.255.255.0
    set default-gateway 192.168.33.1
    set dns-server1 56.34.56.96
    set dns-server2 56.34.56.99
    set lease-time 4000
    set wins-server1 192.168.33.45
  end
```

The following command shows how to add an exclusion range from 192.168.20.22 to 192.168.20.25.

```
config system dhcp server
  edit new_dhcp
    config exclude-range
      edit 1
        set start-ip 192.168.20.22
        set end-ip 192.168.20.25
      end
  end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v2.80 MR2	Added domain field. Removed discard-age field.
FortiOS v2.80 MR8	default-router changed to default-gateway config exclude_range subcommand added (formerly config dhcp exclude_range command)
FortiOS v3.0	Changed exclude_range to exclude-range.
FortiOS v3.0 MR1	Removed edit field.
FortiOS v3.0 MR3	Added edit field.
FortiOS v3.0 MR5	Added conflicted-ip-timeout field.
FortiOS v3.0 MR6	Added ipsec-lease-hold field.

Related topics

- system dhcp reserved-address
- system interface

dns

Use this command to set the DNS server addresses. Several FortiGate functions, including sending email alerts and URL blocking, use DNS.

Syntax

```
config system dns
  set cache-notfound-responses {enable | disable}
  set dns-cache-limit <integer>
  set dns-cache-ttl <int>
  set domain <domain_name>
  set ip6-primary <dns_ipv6>
  set ip6-secondary <dns_ip6>
  set primary <dns_ipv4>
  set secondary <dns_ip4>
end
```

Variable	Description	Default
`cache-notfound-responses {enable | disable}`	Enable to cache NOTFOUND responses from the DNS server.	`disable`
`dns-cache-limit <integer>`	Set maximum number of entries in the DNS cache.	`5000`
`dns-cache-ttl <int>`	Enter the duration, in seconds, that the DNS cache retains information.	`1800`
`domain <domain_name>`	Set the local domain name (optional).	No default.
`ip6-primary <dns_ipv6>`	Enter the primary IPv6 DNS server IP address.	`::`
`ip6-secondary <dns_ip6>`	Enter the secondary IPv6 DNS server IP address.	`::`
`primary <dns_ipv4>`	Enter the primary DNS server IP address.	`65.39.139.53`
`secondary <dns_ip4>`	Enter the secondary DNS IP server address.	`65.39.139.63`

Example

This example shows how to set the primary FortiGate DNS server IP address to `45.37.121.76` and the secondary FortiGate DNS server IP address to `45.37.121.77`.

```
config system dns
  set primary 45.37.121.76
  set secondary 45.37.121.77
end
```

History

FortiOS v2.80 Revised.

FortiOS v2.80 MR2 Added `autosvr` and `fwdintf` fields for models numbered 100 and lower.

FortiOS v2.80 MR8 Added `cache-notfound-responses` field.

FortiOS v3.0 MR7 Added `dns-cache-ttl` field. `autosvr` disabled by default.

FortiOS v4.0 MR1 Removed `autosvr` and `fwdintf` fields.

dns-database

Use this command to configure the FortiGate DNS database so that DNS lookups from an internal network are resolved by the FortiGate DNS database. To configure the DNS database you add zones. Each zone has its own domain name.

You then add entries to each zone. An entry is an host name and the IP address it resolves to. You can also specify if the entry is an IPv4 address (A), an IPv6 address (AAAA), a name server (NS), a canonical name (CNAME), or a mail exchange (MX) name.

Syntax

```
conf system dns-database
  edit <zone-string>
    set domain <domain>
    set ttl <int>
    config dns-entry
      edit <entry-id>
        set canonical-name <canonical_name_string>
        set hostname <hostname_string>
        set ip <ip_address>
        set ipv6 <ipv6_address>
        set preference <preference_value>
        set status {enable | disable}
        set ttl <entry_ttl_value>
        set type {A|AAAA|MX|NS|CNAME}
      end
  end
```

Variable	Description	Default
`edit <zone-string>`	Enter the DNS zone name. This is significant only on the FortiGate unit itself.	No default.
`set domain <domain>`	Set the domain name here -- when matching lookup, use this zone name to match DNS queries	No default.
`set ttl <int>`	Set the packet time-to-live in seconds. Range 0 to 2 147 483 647.	`86400`
`config dns-entry` Variables		
`edit <entry-id>`		
`canonical-name <canonical_name_string>`	Enter the canonical name of the host. This is available if `type` is `CNAME`.	`Null`
`hostname <hostname_string>`	Enter the name of the host.	`Null`
`ip <ip_address>`	Enter the IP address (IPv4) of the host. This is available if `type` is `A`.	`0.0.0.0`
`ipv6 <ipv6_address>`	Enter the IP address (IPv6) of the host. This is available if `type` is `AAAA`.	`::`
`preference <preference_value>`	Enter the preference level. `0` is the highest preference. This is available if `type` is `MX`.	`10`
`status {enable | disable}`	Enable the DNS entry.	`enable`

Variable	Description	Default
`ttl <entry_ttl_value>`	Optionally, override the zone time-to-live value. Range 0 to 2 147 483 647 seconds. `Set to 0` to use zone `ttl` value.	`0`
`type {A|AAAA|MX|NS|CNAME}`	**A** — IPv4 host **AAAA** — IPv6 host **CNAME** — alias **MX** — mail server **NS** — name server	A

Example

This example shows how to add a DNS zone named `Zone_1` and add an IPv4 address entry to the zone.

```
config system dns-database
  edit Zone_1
    set domain example.net
    config dns-entry
      edit 1
        set type A
        set hostname myhost
        set ip 10.10.10.1
      end
  end
```

History

FortiOS 4.0 MR1 New

fips-cc

Use this command to set the FortiGate unit into FIPS-CC mode.

Enable Federal Information Processing Standards-Common Criteria (FIPS-CC) mode. This is an enhanced security mode that is valid only on FIPS-CC-certified versions of the FortiGate firmware.

When switching to FIPS-CC mode, you will be prompted to confirm, and you will have to login.

Note: When you enable FIPS-CC mode, all of the existing configuration is lost.

For more information on FIPS-CC mode, see the FIPS-CC technote on the Knowledge Center website.

Syntax

```
config system fips-cc
  set status <enable | disable>
end
```

Variable	Description	Default
`status <enable | disable>`	Enable to select FIPS-CC mode operation for the FortiGate unit.	`disable`

History

FortiOS v3.0 MR6 Command moved from `config system global set CC-mode`.

fortiguard

Use this command to configure communications with the FortiGuard Distribution Network (FDN) for FortiGuard subscription services such as:

- FortiGuard Antivirus and IPS
- FortiGuard Web Filtering and Antispam
- FortiGuard Analysis and Management Service

For FortiGuard Antivirus and IPS, Web Filtering and Antispam, you can alternatively use this command to configure the FortiGate unit to communicate with a FortiManager system, which can act as a private FortiGuard Distribution Server (FDS) for those services.

By default, FortiGate units connect to the FDN using a set of default connection settings. You can override these settings to use IP addresses and port numbers other than the defaults. For example, if you have a FortiManager unit, you might download a local copy of FortiGuard service updates to the FortiManager unit, then redistribute those updates by configuring each FortiGate unit's server override feature to connect to the FortiManager unit's private FDS IP address. For more information about configuring the FortiManager system to act as a private FDS, see the FortiManager Administration Guide.

IP address and port number overrides for FortiGuard Analysis and Management Service are configured separately from other FortiGuard services. For more information, see "system fortiguard-log" on page 422. For additional information on the FortiGuard Analysis and Management Service, see the *FortiGuard Analysis and Management Service Administration Guide*.

Note: If the FortiGate unit is unable to connect to the FDN, verify connectivity on required ports. For a list of required ports, see the Fortinet Knowledge Center article Traffic Types and TCP/UDP Ports Used by Fortinet Products.

Remote administration by a FortiManager system is mutually exclusive with remote administration by FortiGuard Analysis and Management Service. For information about configuring remote administration by a FortiManager system instead, see "system central-management" on page 406.

Syntax

```
config system fortiguard
  set hostname <url_str>
  set port {53 | 8888}
  set srv-ovrd {enable | disable}
  set client-override-ip <ovrd_ipv4>
  set client-override-status {enable | disable}
  set service-account-id <id_str>
  set load-balance-servers <number>
  set analysis-service {enable | disable}
  set antispam-status {enable | disable}
  set antispam-cache {enable | disable}
  set antispam-cache-ttl <ttl_int>
  set antispam-cache-mpercent <ram_int>
  set antispam-timeout <timeout_int>
  set avquery-status {enable | disable}
  set avquery-cache {enable | disable}
  set avquery-cache-ttl <ttl_int>
  set avquery-cache-mpercent <max_int>
  set avquery-timeout <timeout_int>
  set central-mgmt-auto-backup {enable | disable}
  set central-mgmt-scheduled-config-restore {enable | disable}
  set central-mgmt-scheduled-upgrade {enable | disable}
```

```
    set central-mgmt-status {enable | disable}
    set webfilter-cache {enable | disable}
    set webfilter-cache-ttl <ttl_int>
    set webfilter-status {enable | disable}
    set webfilter-timeout <timeout_int>
    config serv-ovrd-list
      edit <index_int>
        set addr-type {ipv6 | ipv4}
        set ip <ovrd_ipv4>
        set ip6 <ovrd_ipv6>
      end
    end
  end
```

Variable	Description	Default
`hostname <url_str>`	Enter the host name of the primary FortiGuard server. FortiGate unit defaults include the host name. Use this command only when required to change the host name. Alternatively configure `srv-ovrd`. This field is available only if `srv-ovrd` is `disable`.	`service.fortiguard.net`
`port {53 | 8888}`	Enter the port to use for rating queries to the FortiGuard Web Filtering or FortiGuard Antispam service.	`53`
`srv-ovrd {enable | disable}`	Enable to override the primary FortiGuard server set in `hostname`. Specify override server(s) using `config srv-ovrd-list`. Alternatively, configure `hostname`. `hostname` is not used and unavailable for configuration when this field is `enable`.	`disable`
`client-override-ip <ovrd_ipv4>`	Enter the IP address on this FortiGate unit that will be used to connect to the FortiGuard servers. This field is available only if `client-override-status` is `enable`.	No default.
`client-override-status {enable | disable}`	Enable to force your FortiGate unit to connect to the FortiGuard servers using a specific IP address. You must also configure `client-override-ip`.	`disable`
`service-account-id <id_str>`	Enter the Service Account ID to use with communications with FortiGuard Analysis Service or FortiGuard Management Service.	No default.
`load-balance-servers <number>`	Enter the number of FortiGuard servers to connect to. By default, the FortiGate unit always uses the first server in its FortiGuard server list to connect to the FortiGuard network and `load-balance-servers` is set to `1`. You can increase this number up to 20 if you want the FortiGate unit to use a different FortiGuard server each time it contacts the FortiGuard network. If you set `load-balance-servers` to 2, the FortiGate unit alternates between checking the first two servers in the FortiGuard server list.	`1`
`analysis-service {enable | disable}`	Enable or disable for the FortiGuard Analysis and Management Service.	`disable`
`antispam-status {enable | disable}`	Enable or disable use of FortiGuard Antispam.	`disable`
`antispam-cache {enable | disable}`	Enable or disable caching of FortiGuard Antispam query results, including IP address and URL block list. Enabling the cache can improve performance because the FortiGate unit does not need to access the FDN or FortiManager unit each time the same IP address or URL appears as the source of an email. When the cache is full, the least recently used cache entry is replaced.	`disable`

Variable	Description	Default
antispam-cache-ttl <ttl_int>	Enter a time to live (TTL), in seconds, for antispam cache entries. When the TTL expires, the cache entry is removed, requiring the FortiGate unit to query the FDN or FortiManager unit the next time that item occurs in scanned traffic. Valid TTL ranges from 300 to 86400 seconds.	1800
antispam-cache-mpercent <ram_int>	Enter the maximum percentage of memory (RAM) to use for antispam caching. Valid percentage ranges from 1 to 15.	2
antispam-expiration	The expiration date of the FortiGuard Antispam service contract. This variable can be viewed with the get command, but cannot be set.	N/A
antispam-license	The interval of time between license checks for the FortiGuard Antispam service contract. This variable can be viewed with the get command, but cannot be set.	7
antispam-timeout <timeout_int>	Enter the FortiGuard Antispam query timeout. Valid timeout ranges from 1 to 30 seconds.	7
avquery-status {enable | disable}	Enable or disable use of FortiGuard Antivirus.	disable
avquery-cache {enable | disable}	Enable or disable caching of FortiGuard Antivirus query results. Enabling the cache can improve performance because the FortiGate unit does not need to access the FDN each time the same IP address or URL appears as the source of an email. When the cache is full, the least recently used cache entry is replaced.	enable
avquery-cache-ttl <ttl_int>	Enter a time to live (TTL), in seconds, for antivirus cache entries. When the TTL expires, the cache entry is removed, requiring the FortiGate unit to query the FDN or FortiManager unit the next time that item occurs in scanned traffic. Valid TTL ranges from 300 to 86400 seconds.	1800
avquery-cache-mpercent <max_int>	Enter the maximum memory to be used for FortiGuard Antivirus query caching. Valid percentage ranges from 1 to 15.	2
avquery-license	The interval of time between license checks for the FortiGuard Antivirus service contract. This variable can be viewed with the get command, but cannot be set.	Unknown
avquery-expiration	The expiration date of the FortiGuard Antivirus service contract. This variable can be viewed with the get command, but cannot be set.	N/A
avquery-timeout <timeout_int>	Enter the time limit in seconds for the FortiGuard Antivirus service query timeout. Valid timeout ranges from 1 to 30.	7
central-mgmt-auto-backup {enable | disable}	Enable automatic backup of the FortiGate unit's configuration to FortiGuard Analysis and Management Service upon an administrator's logout or session timeout. This field is available only if central-mgmt-status is enable.	disable
central-mgmt-scheduled-config-restore {enable | disable}	Enable scheduled restoration of the FortiGate unit's configuration from FortiGuard Analysis and Management Service. This field is available only if central-mgmt-status is enable.	disable
central-mgmt-scheduled-upgrade {enable | disable}	Enable scheduled upgrades of the FortiGate unit's firmware by FortiGuard Analysis and Management Service. This field is available only if central-mgmt-status is enable.	disable

Variable	Description	Default
central-mgmt-status {enable | disable}	Enable remote administration of the FortiGate unit by FortiGuard Analysis and Management Service. You must also configure service-account-id. For more information about validating or updating the FortiGuard Analysis and Management contract, see "execute fortiguard-log update" on page 704.	disable
webfilter-cache {enable | disable}	Enable or disable caching of FortiGuard Web Filtering query results, including category ratings for URLs. Enabling the cache can improve performance because the FortiGate unit does not need to access the FDN or FortiManager unit each time the same IP address or URL is requested. When the cache is full, the least recently used cache entry is replaced.	disable
webfilter-cache-ttl <ttl_int>	Enter a time to live (TTL), in seconds, for web filtering cache entries. When the TTL expires, the cache entry is removed, requiring the FortiGate unit to query the FDN or FortiManager unit the next time that item occurs in scanned traffic. Valid TTL ranges from 300 to 86400 seconds.	3600
webfilter-expiration	The expiration date of the FortiGuard Web Filtering service contract. This variable can be viewed with the get command, but cannot be set.	N/A
webfilter-license	The interval of time between license checks for the FortiGuard Web Filtering service contract. Initially, this value is unknown, and is set after contacting the FDN to validate the FortiGuard Web Filtering license. This variable can be viewed with the get command, but cannot be set.	Unknown
webfilter-status {enable | disable}	Enable or disable use of FortiGuard Web Filtering service.	disable
webfilter-timeout <timeout_int>	Enter the FortiGuard Web Filtering query timeout. Valid timeout ranges from 1 to 30 seconds.	15
config serv-ovrd-list This command is available only if srv-ovrd is enable.		
<index_int>	Enter the index number of a FortiGuard Antivirus and IPS server override.	No default.
addr-type {ipv6 | ipv4}	Select whether IPv4 or IPv6 addresses will be used.	ipv4
ip <ovrd_ipv4>	Enter the IP address that will override the default server IP address. This may be the IP address of a FortiManager unit or a specific FDN server. This is available when addr-type is ipv4.	0.0.0.0
ip6 <ovrd_ipv6>	Enter the IP address that will override the default server IP address. This may be the IP address of a FortiManager unit or a specific FDN server. This is available when addr-type is ipv6.	::

Example

This example shows how to configure the FortiGate unit for remote administration by FortiGuard Analysis and Management Service.

```
config system fortiguard
  set central-mgmt-status enable
  set service-account-id ExampleCo
  set central-mgmt-auto-backup enable
  set central-mgmt-config-restore enable
  set central-mgmt-scheduled-upgrade enable
```

```
end
config system management-tunnel
end
```

History

FortiOS v3.0	New.
FortiOS v3.0 MR2	Added `get system fortiguard-service status` command reference.
FortiOS v3.0 MR5	Added `service-account id`, `central-mgmt-status`, `central-mgmt-schedule-upgrade`, `central-mgmt-auto-backup`, and `central-mgmt-scheduled-config-restore` for FortiGuard Analysis and Management Service and future FortiManager system features.
FortiOS v3.0 MR7	Added `load-balance-servers` field and the `analysis-service` field.
FortiOS v4.0 MR1	Added `addr-type`, `ip6`.

Related topics

- get system dashboard
- system fortiguard-log
- system central-management
- fortiguard setting

fortiguard-log

Use this command to override default ports and IP addresses that the FortiGate unit connects to for FortiGuard Analysis and Management Service.

Syntax

```
config system fortiguard-log
  set controller-ip <address_ipv4>
  set controller-port <port_int>
  set override-controller {enable | disable}
end
```

Variable	Description	Default
`controller-ip <address_ipv4>`	Enter the IP address of the FortiGuard Analysis and Management Service controller. This option appears only if `override-controller` is `enable`.	`0.0.0.0`
`controller-port <port_int>`	Enter the port number of the FortiGuard Analysis and Management Service controller. Valid ports range from 0 to 65535. This option appears only if `override-controller` is `enable`.	`0`
`override-controller {enable | disable}`	Select to override the default FortiGuard Analysis and Management Service controller IP address and/or port.	`disable`

Example

This example shows how to override the default IP address and port number to which the FortiGate unit connects when communicating with the FortiGuard Analysis and Management Service for features such as remote logging and reporting.

```
config system fortiguard-log
  set override-controller enable
  set controller-ip 172.16.21.155
  set controller-port 1234
end
```

History

FortiOS v3.0 MR4 New.

Related topics

- system fortiguard
- fortiguard setting

global

Use this command to configure global settings that affect various FortiGate systems and configurations.

Runtime-only config mode was introduced in FortiOS v3.0 MR2. This mode allows you to try out commands that may put your FortiGate unit into an unrecoverable state normally requiring a physical reboot. In runtime-only config mode you can set a timeout so after a period of no input activity the FortiGate unit will reboot with the last saved configuration. Another option in runtime-only configuration mode is to manually save your configuration periodically to preserve your changes. For more information see `set cfg-save {automatic | manual | revert}`, `set cfg-revert-timeout <seconds>`, and `execute cfg reload`.

Switch mode is available on FortiWiFi 60B, FortiGate 60B, FortiGate 100A (Rev2.0 and higher), and FortiGate 200A (Rev2.0 and higher) models where the internal interface is a four or six port switch. Normally the internal interface is configured as one interface shared by all four ports. Switch mode allows you to configure each interface on the switch separately with their own interfaces. A VLAN can not be configured on a switch interface. Consult your release notes for the most current list of supported models for this feature. The fields `internal-switch-mode {hub | interface | switch}` and `internal-switch-speed {100full | 100half | 10full | 10half | auto}` apply only to switch mode enabled FortiGate models.

Syntax

```
config system global
  set access-banner {enable | disable}
  set admin-https-pki-required {enable | disable}
  set admin-lockout-duration <time_int>
  set admin-lockout-threshold <failed_int>
  set admin-maintainer {enable | disable}
  set admin-port <port_number>
  set admin-scp {enable | disable}
  set admin-server-cert { self-sign | <certificate> }
  set admin-sport <port_number>
  set admin-ssh-port <port_number>
  set admin-ssh-v1 {enable | disable}
  set admin-telnet-port <port_number>
  set admintimeout <admin_timeout_minutes>
  set anti-replay {disable  | loose | strict}
  set auth-cert <cert-name>
  set auth-http-port <http_port>
  set auth-https-port <https_port>
  set auth-keepalive {enable | disable}
  set auth-policy-exact-match {enable | disable}
  set av-failopen {idledrop | off | one-shot | pass}
  set av-failopen-session {enable | disable}
  set batch-cmdb {enable | disable}
  set cfg-save {automatic | manual | revert}
  set cfg-revert-timeout <seconds>
  set check-protocol-header {loose | strict}
  set check-reset-range {enable | disable}
  set clt-cert-req {enable | disable}
  set daily-restart {enable | disable}
  set detection-summary {enable | disable}
  set dst {enable | disable}
  set endpoint-control-portal-port <endpoint_port>
```

```
    set failtime <failures_count>
    set fds-statistics {enable | disable}
    set fds-statistics-period <minutes>
    set fortiswitch-heartbeat {enable | disable}
    set fsae-burst-size <packets>
    set fsae-rate-limit (pkt_sec)
    set gui-ipv6 {enable | disable}
    set gui-lines-per-page <gui_lines>
    set hostname <unithostname>
    set http-obfuscate {header-only | modified | no-error | none}
    set ie6workaround {enable | disable}
    set internal-switch-mode {hub | interface | switch}
    set internal-switch-speed {100full | 100half | 10full | 10half | auto}
    set interval <deadgw_detect_seconds>
    set ip-src-port-range <start_port>-<end_port>
    set language <language>
    set lcdpin <pin_number>
    set lcdprotection {enable | disable}
    set ldapconntimeout <ldaptimeout_msec>
    set loglocaldeny {enable | disable}
    set management-vdom <domain>
    set optimize {antivirus | throughput}
    set phase1-rekey {enable | disable}
    set radius-port <radius_port>
    set refresh <refresh_seconds>
    set registration-notification {disable | enable}
    set remoteauthtimeout <remoteauth_timeout_mins>
    set reset-sessionless-tcp {enable | disable}
    set restart-time <hh:mm>
    set send-pmtu-icmp {enable | disable}
    set service-expire-notification {disable | enable}
    set show-backplane-intf {enable | disable}
    set sslvpn-sport <port_number>
    set strong-crypto {enable | disable}
    set syncinterval <ntpsync_minutes>
    set tcp-halfclose-timer <seconds>
    set tcp-halfopen-timer <seconds>
    set tcp-option {enable | enable}
    set tcp-timewait-timer <seconds_int>
    set timezone <timezone_number>
    set tos-based-priority {low | medium | high}
    set tp-mc-skip-policy {enable | disable}
    set udp-idle-timer <seconds>
    set user-server-cert <cert_name>
    set vdom-admin {enable | disable}
    set vip-arp-range {unlimited | restricted}
    set wireless-controller {enable | disable}
    set wireless-controller-port <port_int>
    set wireless-terminal {enable | disable}
    set wireless-terminal-port <port_int>
end
```

Variable	Description	Default
access-banner {enable | disable}	Enable to display the admin access disclaimer message. For more information see “system replacemsg admin” on page 477.	disable
admin-https-pki-required {enable | disable}	Enable to allow user to login by providing a valid certificate if PKI is enabled for HTTPS administrative access. Default setting disable allows admin users to log in by providing a valid certificate or password.	disable
admin-lockout-duration <time_int>	Set the administration account’s lockout duration in seconds for the firewall. Repeated failed login attempts will enable the lockout. Use admin-lockout-threshold to set the number of failed attempts that will trigger the lockout.	60
admin-lockout-threshold <failed_int>	Set the threshold, or number of failed attempts, before the account is locked out for the admin-lockout-duration.	3
admin-maintainer {enable | disable}	Enabled by default. Disable for CC.	enable
admin-port <port_number>	Enter the port to use for HTTP administrative access.	80
admin-scp {enable | disable}	Enable to allow system configuration download by the secure copy (SCP) protocol.	disable
admin-server-cert { self-sign | <certificate> }	Select the admin https server certificate to use. Choices include self-sign, and the filename of any installed certificates. Default setting is Fortinet_Factory, if available, otherwise self-sign.	See definition under Description.
admin-sport <port_number>	Enter the port to use for HTTPS administrative access.	443
admin-ssh-port <port_number>	Enter the port to use for SSH administrative access.	22
admin-ssh-v1 {enable | disable}	Enable compatibility with SSH v1.0.	disable
admin-telnet-port <port_number>	Enter the port to use for telnet administrative access.	21
admintimeout <admin_timeout_minutes>	Set the number of minutes before an idle administrator times out. This controls the amount of inactive time before the administrator must log in again. The maximum admintimeout interval is 480 minutes (8 hours). To improve security keep the idle timeout at the default value of 5 minutes.	5
anti-replay {disable | loose | strict}	Set the level of checking for packet replay. One of: **disable** — No anti-replay checking. **loose** — Performs packet sequence checking and ICMP anti-replay checking. **strict** — Performs all of the loose checking and also drops SYN packets after the connection has been established with the remote system. This will help prevent a SYN flood and free up system resources.	strict
auth-cert <cert-name>	Https server certificate for policy authentication. Self-sign is the built in certificate but others will be listed as you add them.	self-sign
auth-http-port <http_port>	Set the HTTP authentication port. <http_port> can be from 1 to 65535.	1000
auth-https-port <https_port>	Set the HTTPS authentication port. <https_port> can be from 1 to 65535.	1003
auth-keepalive {enable | disable}	Enable to extend the authentication time of the session through periodic traffic to prevent an idle timeout.	disable

Variable	Description	Default
auth-policy-exact-match {enable | disable}	Enable to require traffic to exactly match an authenticated policy with a policy id and IP address to pass through. When disabled, only the IP needs to match.	disable
av-failopen {idledrop | off | one-shot | pass}	Set the action to take if there is an overload of the antivirus system. Valid options are off, one-shot, and pass. **idledrop** — drop connections based on the clients that have the most connections open. This is most useful for Windows applications, and can prevent malicious bots from keeping an idle connection open to a remote server. **off** — stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions. **one-shot** — bypass the antivirus system when memory is low. You must enter off or pass to restart antivirus scanning. **pass** — bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved. This applies to FortiGate models numbered 300A and higher.	pass
av-failopen-session {enable | disable}	When enabled and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by av-failopen. This applies to models numbered 300A and higher.	disable
batch-cmdb {enable | disable}	Enable/disable batch mode. Batch mode is used to enter a series of commands, and executing the commands as a group once they are loaded. For more information, see "execute batch" on page 689.	enable
cfg-save {automatic | manual | revert}	Set the method for saving the FortiGate system configuration and enter into runtime-only configuration mode. Methods for saving the configuration are: **automatic** — automatically save the configuration after every change. **manually** — manually save the configuration using the execute cfg save command. **revert** — manually save the current configuration and then revert to that saved configuration after cfg-revert-timeout expires. Switching to automatic mode disconnects your session. This command is used as part of the runtime-only configuration mode. See "execute cfg reload" on page 691 for more information.	automatic
cfg-revert-timeout <seconds>	Enter the timeout interval in seconds. If the administrator makes a change and there is no activity for the timeout period, the FortiGate unit will automatically revert to the last saved configuration. Default timeout is 600 seconds. This command is available only when cfg-save is set to revert. This command is part of the runtime-only configuration mode. See "execute cfg reload" on page 691 for more information.	600
check-reset-range {enable | disable}	Set whether RST out-of-window checking is performed. If set to strict (enable), RST must fall between the last ACK and the next send. If set to disable, no check is performed.	disable
check-protocol-header {loose | strict}	Select the level of checking performed on protocol headers.	loose
clt-cert-req {enable | disable}	Enable to require a client certificate before an administrator logs on to the web-based manager using HTTPS.	disable

Variable	Description	Default
daily-restart {enable | disable}	Enable to restart the FortiGate unit every day. The time of the restart is controlled by restart-time.	disable
detection-summary {enable | disable}	Disable to prohibit the collection of detection summary statistics for FortiGuard.	enable
dst {enable | disable}	Enable or disable daylight saving time. If you enable daylight saving time, the FortiGate unit adjusts the system time when the time zone changes to daylight saving time and back to standard time.	disable
endpoint-control-portal-port <endpoint_port>	Enter the port number from 1 to 65535 for the endpoint control portal port for FortiClient downloads.	8009
failtime <failures_count>	Set the dead gateway detection failover interval. Enter the number of times that ping fails before the FortiGate unit assumes that the gateway is no longer functioning. 0 disables dead gateway detection.	5
fds-statistics {enable | disable}	Enable or disable AV/IPS signature reporting. If necessary, disable to avoid error messages on HA subordinate units during an AV/IPS update.	enable
fds-statistics-period <minutes>	Select the number of minutes in the FDS report period. Range is 1 to 1440 minutes.	60
fortiswitch-heartbeat {enable | disable}	Enable or disable sending heartbeat packets from FortiGate unit backplane fabric interfaces. This field is only available for FortiGate-5001A and FortiGate-5005FA2 boards. A FortiSwitch-5003A board receives the heartbeat packets to verify that the FortiGate board is still active. The FortiGate board sends 10 packets per second from each fabric interface. The packets are type 255 bridge protocol data unit (BPDU) packets.	disable
fsae-burst-size <packets>	Set the FSAE burst size in packets.	300
fsae-rate-limit (pkt_sec)	Set the FSAE message rate limit in packets per second.	100
gui-ipv6 {enable | disable}	Enable or disable ability to configure IPv6 using the web-based manager.	disable
gui-lines-per-page <gui_lines>	Set the number of lines displayed on table lists. Range is from 20 - 1000 lines per page.	50
hostname <unithostname>	Enter a name to identify this FortiGate unit. A hostname can only include letters, numbers, hyphens, and underlines. No spaces are allowed. While the hostname can be longer than 16 characters, if it is longer than 16 characters it will be truncated and end with a "~" to indicate it has been truncated. This shortened hostname will be displayed in the CLI, and other locations the hostname is used. FortiGate 5000 models support longer hostnames - some up to 35 characters. By default the hostname of your FortiGate unit is its serial number which includes the model.	FortiGate serial number.
http-obfuscate {header-only | modified | no-error | none}	Set the level at which the identity of the FortiGate web server is hidden or obfuscated. **none** — do not hide the FortiGate web server identity. **header-only** — hides the HTTP server banner. **modified** — provides modified error responses. **no-error** — suppresses error responses.	none
ie6workaround {enable | disable}	Enable or disable the work around for a navigation bar freeze issue caused by using the FortiGate web-based manager with Internet Explorer 6.	disable

Variable	Description	Default
internal-switch-mode {hub | interface | switch}	Set the mode for the internal switch to be one of hub, interface, or switch. Switch mode combines FortiGate unit interfaces into one switch with one address. Interface mode gives each internal interface its own address. On some FortiGate models you can also select *Hub Mode*. Hub mode is similar to switch mode except that in hub mode the interfaces do not learn the MAC addresses of the devices on the network they are connected to and may also respond quicker to network changes in some circumstances. You should only select *Hub Mode* if you are having network performance issues when operating with switch mode. The configuration of the FortiGate unit is the same whether in switch mode or hub mode. Before switching modes, all configuration settings for the interfaces affected by the switch must be set to defaults.	switch
internal-switch-speed {100full | 100half | 10full | 10half | auto}	Set the speed of the switch used for the internal interface. Choose one of: **100full** **100half** **10full** **10half** **auto** 100 and 10 refer to 100M or 10M bandwidth. Full and half refer to full or half duplex. Default value is auto. This applies only to FortiWiFi 60B, FortiGate 60B, 100A (Rev2.0 and higher), and 200A (Rev2.0 and higher) models.	auto
interval <deadgw_detect_seconds>	Select the number of seconds between pings the FortiGate unit sends to the target for dead gateway detection. Selecting 0 disables dead gateway detection.	5
ip-src-port-range <start_port>-<end_port>	Specify the IP source port range used for traffic originating from the FortiGate unit. The valid range for <start_port> and <end_port> is from 1 to 65535 inclusive. You can use this setting to avoid problems with networks that block some ports, such as FDN ports.	1024-4999
language <language>	Set the web-based manager display language. You can set <language> to one of english, french, japanese, korean, portuguese, spanish, simch (Simplified Chinese) or trach (Traditional Chinese).	english
lcdpin <pin_number>	Set the 6 digit PIN administrators must enter to use the LCD panel. This applies to FortiGate models numbered 300 to 3600.	123456
lcdprotection {enable | disable}	Enable or disable LCD panel PIN protection. This applies to FortiGate models numbered 300 to 3600.	disable
ldapconntimeout <ldaptimeout_msec>	LDAP connection timeout in msec	500
loglocaldeny {enable | disable}	Enable or disable logging of failed connection attempts to the FortiGate unit that use TCP/IP ports other than the TCP/IP ports configured for management access (443 for https, 22 for ssh, 23 for telnet, and 80 for HTTP by default).	disable
log-user-in-upper {enable | disable}	Log username in uppercase letters.	disable
management-vdom <domain>	Enter the name of the management virtual domain. Management traffic such as FortiGuard traffic originates from the management VDOM.	root

Variable	Description	Default
optimize {antivirus | throughput}	Set firmware performance optimization to either antivirus or throughput. This is available on FortiGate models numbered 1000 and higher.	antivirus
phase1-rekey {enable | disable}	Enable or disable automatic rekeying between IKE peers before the phase 1 keylife expires.	enable
radius-port <radius_port>	Change the default RADIUS port. The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645 you can use the CLI to change the default RADIUS port on your FortiGate unit.	1812
refresh <refresh_seconds>	Set the Automatic Refresh Interval, in seconds, for the web-based manager System Status Monitor. Enter 0 for no automatic refresh.	0
registration-notification {disable | enable}	Enable or disable displaying the registration notification on the web-based manager if the FortiGate unit is not registered.	enable
remoteauthtimeout <remoteauth_timeout_mins>	Timeout for RADIUS/LDAP authentication in minutes. To improve security keep the remote authentication timeout at the default value of 5 minutes.	5
reset-sessionless-tcp {enable | disable}	Enabling this option may help resolve issues with a problematic server, but it can make the FortiGate unit more vulnerable to denial of service attacks. In most cases you should leave reset-sessionless-tcp disabled. The reset-sessionless-tcp command determines what action the FortiGate unit performs if it receives a TCP packet but cannot find a corresponding session in its session table. This happens most often because the session has timed out. If you disable reset-sessionless-tcp, the FortiGate unit silently drops the packet. The packet originator does not know that the session has expired and might re-transmit the packet several times before attempting to start a new session. This is normal network operation. If you enable reset-sessionless-tcp, the FortiGate unit sends a RESET packet to the packet originator. The packet originator ends the current session, but it can try to establish a new session. This is available in NAT/Route mode only.	disable
restart-time <hh:mm>	Enter daily restart time in hh:mm format (hours and minutes). This is available only when daily-restart is enabled.	No default.
send-pmtu-icmp {enable | disable}	Select enable to send a path maximum transmission unit (PMTU) - ICMP destination unreachable packet. Enable if you need to support PTMUD protocol on your network to reduce fragmentation of packets. Disabling this command will likely result PMTUD packets being blocked by the unit.	
service-expire-notification {disable | enable}	Enable or disable displaying a notification on the web-based manager 30 days before the FortiGate unit support contract expires.	enable
show-backplane-intf {enable | disable}	Select enable to show FortiGate-5000 backplane interfaces as port9 and port10. Once these backplanes are visible they can be treated as regular physical interfaces. This is only available on FortiGate-5000 models.	disable
sslvpn-sport <port_number>	Enter the port to use for SSL-VPN access (HTTPS).	443

Variable	Description	Default
strong-crypto {enable | disable}	Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta). Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption.	disable
syncinterval <ntpsync_minutes>	Enter how often, in minutes, the FortiGate unit should synchronize its time with the Network Time Protocol (NTP) server. The syncinterval number can be from 1 to 1440 minutes. Setting to 0 disables time synchronization.	0
tcp-halfclose-timer <seconds>	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds.	120
tcp-halfopen-timer <seconds>	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds.	60
tcp-option {enable | enable}	Enable SACK, timestamp and MSS TCP options. For normal operation tcp-option should be enabled. Disable for performance testing or in rare cases where it impairs performance.	enable
tcp-timewait-timer <seconds_int>	Set the length of the TCP TIME-WAIT state in seconds. As described in RFC 793, the “TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request”. Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached. The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds	120
timezone <timezone_number>	The number corresponding to your time zone from 00 to 72. Press ? to list time zones and their numbers. Choose the time zone for the FortiGate unit from the list and enter the correct number.	00
tos-based-priority {low | medium | high}	Select the default system-wide level of priority for Type of Service (TOS). TOS determines the priority of traffic for scheduling. Typically this is set on a per service type level. For more information, see “system tos-based-priority” on page 532. The value of this field is the default setting for when TOS is not configured on a per service level.	high
tp-mc-skip-policy {enable | disable}	Enable to allow skipping of the policy check, and to enable multicast through.	disable
udp-idle-timer <seconds>	Enter the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds.	180
user-server-cert <cert_name>	Select the certificate to use for https user authentication. Default setting is Fortinet_Factory, if available, otherwise self-sign.	See definition under Description.
vdom-admin {enable | disable}	Enable to configure multiple virtual domains.	disable

Variable	Description	Default
vip-arp-range {unlimited | restricted}	vip-arp-range controls the number of ARP packets the FortiGate unit sends for a VIP range. If restricted, the FortiGate unit sends ARP packets for only the first 8192 addresses in a VIP range. If unlimited, the FortiGate unit sends ARP packets for every address in the VIP range.	restricted
wireless-controller {enable | disable}	Enable wireless controller feature.	disable
wireless-controller-port <port_int>	Select the port used for the control channel in wireless controller mode. The range is 1024 through 49150. This is not available on FortiWiFi units. The data channel port is the control channel port number plus one.	5246
wireless-terminal {enable | disable}	Enable this FortiWiFi unit to be managed by another FortiGate unit's wireless controller feature. This is available only on FortiWiFi units. In wireless terminal mode, the wireless functionality of the FortiWiFi unit cannot be controlled from the unit itself.	disable
wireless-terminal-port <port_int>	Select the port used for the control channel in wireless terminal mode. The range is 1024 through 49150. This is available only on FortiWiFi units. The data channel port is the control channel port number plus one.	5246

Example

This example shows how to change to enable daylight savings time.

```
config system global
  set dst enable
end
```

History

FortiOS v2.80 New.

FortiOS v2.80 MR2 The ip-overlap field was changed to allow-interface-subnet-overlap.

FortiOS v2.80 MR3 Added av_failopen and reset_sessionless_tcp fields.

FortiOS v2.80 MR4 Moved date and time to execute branch.
Added phase1-rekey field.

FortiOS v2.80 MR6 Added ips-open field.

FortiOS v3.0 Removed management-vdom, opmode fields.
Added detection-summary, fsae-burst-size, fsae-rate-limit, ldapconntimeout, remoteauthtimeout.
Changed underscore to hyphen in av-failopen, conn-tracking, ip_signature, local_anomaly, mc-ttl-notchange, radius-port, reset-sessionless-tcp, restart-time, tcp-option.

FortiOS v3.0 MR1 Removed sslvpn-enable field.
Added av-failopen-session, management-vdom, strong-crypto fields.

FortiOS v3.0 MR2 Added admin-ssh-port, admin-telnet-port, cfg-save, cfg-revert-timeout, tcp-halfopen-timer, tos-based-priority.

FortiOS v3.0 MR3 Added fds-statistics and udp-idle-timer. Removed mc-ttl-notchange, batch_sleep, and multicast-forward.

FortiOS v3.0 MR4 Added access-banner, admin-server-cert, admin-telnet-port, forticlient-portal-port and tcp-halfopen-timer. Removed asymroute.

FortiOS v3.0 MR5 Added admin-https-pki-required, admin-maintainer, user-server-cert, internal-switch-mode, internal-switch-speed, forticlient-portal-port, tp-mc-skip-policy. Added auth-cert command.

FortiOS v3.0 MR6	Modified definition of `admin-server-cert` and `user-server-cert`. Removed `local-anomaly, and CC-mode`. Moved `authtimeout, auth-secure-http, and auth-type` to `config user settings`. Added new `idledrop` option for `av-failopen` command, and `fds-statistics-period` command. Modified default value of `optimize` field.
FortiOS v3.0 MR7	Removed `allow-interface-subnet-overlap`. Added `tcp-timewait-timer`. Added `fortiswitch-heartbeat`.
FortiOS v3.0 MR7 Patch 1	Added `portuguese` to `language` field
FortiOS v4.0	Added `check-protocol-header, admin-lockout-duration, admin-lockout-threshold`, `endpoint-control-portal-port`, `send-pmtu-icmp, auth-policy-exact-match`. Changed `batch_cmdb` to `batch-cmdb`. Removed `forticlient-check-portal-port`.
FortiOS v4.0 MR1	Added `log-user-in-upper`, `registration-notification`, `service-expire-notification, wireless-controller`. Added the `hub` option of the `internal-switch-mode` field.

Related topics

- execute cfg reload
- execute cfg save

gre-tunnel

Use this command to configure the tunnel for a GRE interface. A new interface of type “tunnel” with the same name is created automatically as the local end of the tunnel. This command is available only in NAT/Route mode.

To complete the configuration of a GRE tunnel, you need to:

- configure a firewall policy to pass traffic from the local private network to the tunnel interface
- configure a static route to the private network at the remote end of the tunnel using the GRE tunnel “device”
- optionally, define the IP addresses for each end of the tunnel to enable dynamic routing through the tunnel or to enable pinging of each end of the tunnel for testing

Syntax

```
config system gre-tunnel
  edit <tunnel_name>
    set interface <interface_name>
    set local-gw <localgw_IP>
    set remote-gw <remotegw_IP>
  end
```

Variable	Description	Default
`edit <tunnel_name>`	Enter a name for the tunnel.	No default.
`interface <interface_name>`	Enter the physical or VLAN interface that functions as the local end of the tunnel.	
`local-gw <localgw_IP>`	Enter the IP address of the local gateway.	
`remote-gw <remotegw_IP>`	Enter the IP address of the remote gateway.	

Example

In this example, a GRE tunnel is needed between two sites using FortiGate units. Users on the 192.168.2.0/24 network at Site A need to communicate with users on the 192.168.3.0/24 network at Site B. At both sites the private network is connected to Port 2 of the FortiGate unit and the connection to the Internet is through Port 1. At Site A, the public IP address is 172.16.67.199 and at Site B it is 172.16.68.198.

Site A configuration

```
config system gre-tunnel
  edit toSiteB
    set interface port1
    set local-gw 172.16.67.199
    set remote-gw 172.16.68.198
  end
```

Site B configuration

```
config system gre-tunnel
  edit toSiteA
    set interface port1
    set local-gw 172.16.68.198
    set remote-gw 172.16.67.199
  end
```

Site A configuration

```
config firewall policy
  edit 1
    set src-intf port2
    set dst-intf toSiteB
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set src-intf toSiteB
    set dst-intf port2
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  end

config route static
  edit 1
    set device toSiteB
    set dst 192.168.3.0/24
  end
```

(Optional)

```
config system interface
  edit toSiteB
    set ip 10.0.0.1/32
    set remote-ip 10.0.0.2
    set allowaccess ping
  end
```

Site B configuration

```
config firewall policy
  edit 1
    set src-intf port2
    set dst-intf toSiteA
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set src-intf toSiteA
    set dst-intf port2
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  end

config route static
  edit 1
    set device toSiteA
    set dst 192.168.2.0/24
  end
```

(Optional)

```
config system interface
  edit toSiteA
    set ip 10.0.0.2/32
    set remote-ip 10.0.0.1
    set allowaccess ping
  end
```

History

FortiOS v3.0 New

Related topics

- system interface
- firewall policy, policy6
- router static

ha

Use this command to enable and configure FortiGate high availability (HA) and virtual clustering. HA is supported on FortiGate and FortiWiFi models numbered 60 and higher. Using the `config system ha` command you must configure all cluster members with the same group name, mode, and password before the FortiGate units can form a cluster.

Group name, mode, password, as well as priority and group ID are not synchronized between cluster units. The primary unit synchronizes all other configuration settings, including the other HA configuration settings.

When virtual domains are enabled for the FortiGate units to be operating in HA mode you are configuring virtual clustering. Using virtual clustering you create two virtual clusters and add virtual domains to each cluster. Configuring virtual clustering is very similar to configuring normal HA except that in a virtual cluster, the HA mode can only be set to active-passive. As well additional options are available for adding virtual domains to each virtual cluster and for setting the device priority for each device in each virtual cluster.

Note: You cannot enable HA mode if one of the FortiGate unit interfaces uses DHCP or PPPoE to acquire an IP address. If DHCP or PPPoE is configured, the `config ha mode` keyword is not available. You also cannot enable HA mode if you have configured standalone session synchronization. See "system session-sync" on page 509.

Note: You cannot enable HA mode if you have configured standalone session synchronization. See "system session-sync" on page 509.

For complete information about how to configure and operate FortiGate HA clusters and more detail about the `config system ha` CLI command, see the *FortiGate HA Overview*, the *FortiGate HA Guide*, and the Fortinet Knowledge Center.

Syntax

```
config system ha
  set arps <arp_integer>
  set arps-interval <interval_integer>
  set authentication {disable | enable}
  set encryption {disable | enable}
  set group-id <id_integer>
  set group-name <name_str>
  set hb-interval <interval_integer>
  set hb-lost-threshold <threshold_integer>
  set hbdev <interface_name> <priority_integer> [<interface_name>
     <priority_integer>]...
  set helo-holddown <holddown_integer>
  set link-failed-signal {disable | enable}
  set load-balance-all {disable | enable}
  set mode {a-a | a-p | standalone}
  set monitor <interface_names>
  set override {disable | enable}
  set password <password_str>
  set pingserver-failover-threshold <threshold_integer>
  set pingserver-flip-timeout <timeout_integer>
  set pingserver-monitor-interface <interface_names>
  set priority <priority_integer>
  set route-hold <hold_integer>
  set route-ttl <ttl_integer>
  set route-wait <wait_integer>
```

```
set schedule {hub | ip | ipport | leastconnection | none | random
   | round-robin | weight-round-robin}
set session-pickup {disable | enable}
set sync-config {disable | enable}
set uninterruptable-upgrade {disable | enable}
set weight <priority_integer> <weight_integer>
set vdom <vdom_names>
set vcluster2 {disable | enable}
end
config secondary-vcluster
  set monitor <interface_names>
  set override {disable | enable}
  set priority <priority_integer>
  set vdom <vdom_names>
  set pingserver-failover-threshold <threshold_integer>
  set pingserver-monitor-interface <interface_names>
  end
end
```

Variable	Description	Default
arps <arp_integer>	Set the number of times that the primary unit sends gratuitous ARP packets. Gratuitous ARP packets are sent when a cluster unit becomes a primary unit (this can occur when the cluster is starting up or after a failover). Gratuitous ARP packets configure connected network devices to associate the cluster virtual MAC addresses and cluster IP address with primary unit physical interfaces. (This is sometimes called using gratuitous ARP packets to train the network.) The arps range is 1 to 16. Normally you would not need to change the arps setting. However you may need to increase the number of times the primary unit sends gratuitous ARP packets if your cluster takes a long time to failover or to train the network. Sending more gratuitous ARP packets may help the failover happen faster. There may be a number of reasons to reduce the number of times that gratuitous ARP packets are sent. For example, if your cluster has a large number of VLAN interfaces and virtual domains and because gratuitous ARP packets are broadcast, sending gratuitous ARP packets may generate a lot of network traffic. As long as the cluster still fails over successfully you could reduce the number of time gratuitous ARP packets are sent to reduce the amount of traffic produced after a failover. Depending on your network, you may be able to use both the arps and the arps-interval fields to improve how quickly your cluster fails over.	5
arps-interval <interval_integer>	Set the number of seconds to wait between sending gratuitous ARP packets. When a cluster unit becomes a primary unit (this occurs when the cluster is starting up or after a failover) the primary unit sends gratuitous ARP packets immediately to inform connected network equipment of the IP address and MAC address of the primary unit. The primary unit then waits for the number of seconds in the arps-interval and sends the gratuitous ARP packets again. This happens until the gratuitous ARP packets have been sent the number of times set by the arps field. The arps-interval range is 1 to 20 seconds. Normally you would not need to change the arps-interval. However, you may need to decrease the arps-interval to send gratuitous ARP packets more often if your cluster takes a long time to failover or to train the network. There may be a number of reasons to set the arps-interval higher. For example, if your cluster has a large number of VLAN interfaces and virtual domains and because gratuitous ARP packets are broadcast, sending gratuitous ARP packets may generate a lot of network traffic. As long as the cluster still fails over successfully you could increase arps-interval to reduce the amount of traffic produced after a failover.	8
authentication {disable | enable}	Enable/disable HA heartbeat message authentication. Enabling HA heartbeat message authentication prevents an attacker from creating false HA heartbeat messages. False HA heartbeat messages could affect the stability of the cluster.	disable
encryption {disable | enable}	Enable/disable HA heartbeat message encryption. Enabling HA heartbeat message encryption prevents an attacker from sniffing HA packets to get HA cluster information.	disable
group-id <id_integer>	The HA group ID. The group ID range is from 0 to 63. All members of the HA cluster must have the same group ID. Changing the Group ID changes the cluster virtual MAC address.	0
group-name <name_str>	The HA group name. All cluster members must have the same group name. The maximum length of the group name is 32 characters.	FGT-HA

Variable	Description	Default
`hb-lost-threshold <threshold_integer>`	The lost heartbeat threshold is the number of consecutive heartbeat packets that are not received from another cluster unit before assuming that the cluster unit has failed. The default value is 6, meaning that if the 6 heartbeat packets are not received from a cluster unit then that cluster unit is considered to have failed. The range is 1 to 60 packets. The lower the `hb-lost-threshold` the faster a cluster responds when a unit fails. However, sometimes heartbeat packets may not be sent because a cluster unit is very busy. This can lead to a false positive failure detection. To reduce these false positives you can increase the `hb-lost-threshold`.	6
`hb-interval <interval_integer>`	The heartbeat interval is the time between sending heartbeat packets. The heartbeat interval range is 1 to 20 (100*milliseconds). So an `hb-interval` of 2 means a heartbeat packet is sent every 200 milliseconds. The `hb-interval` also works with the `hb-lost-threshold` to set how long a cluster unit waits before assuming that another cluster unit has failed and is no longer sending heartbeat packets. For the default configuration, if a cluster unit does not receive a heartbeat packet from a cluster unit for 6 * 200 = 1200 milliseconds or 1.2 seconds the cluster unit assumes that the other cluster unit has failed. You can increase both the `hb-interval` and the `hb-lost-threshold` to reduce false positives. For example, increasing `hb-interval` to 20 and `hb-lost-threshold` to 30 means a failure will be assumed if no heartbeat packets are received after 30 * 2000 milliseconds = 60,000 milliseconds, or 60 seconds.	2
`hbdev <interface_name> <priority_integer> [<interface_name> <priority_integer>]...`	Select the FortiGate interfaces to be heartbeat interfaces and set the heartbeat priority for each interface. The heartbeat interface with the highest priority processes all heartbeat traffic. If two or more heartbeat interfaces have the same priority, the heartbeat interface that with the lowest hash map order value processes all heartbeat traffic. The CLI lists interfaces in alphanumeric order: • port1 • port2 through 9 • port10 Hash map order sorts interfaces in the following order: • port1 • port10 • port2 through port9 By default two interfaces are configured to be heartbeat interfaces and the priority for both these interfaces is set to 50. The heartbeat interface priority range is 0 to 512. In most cases you can maintain the default `hbdev` configuration as long as you can connect the `hbdev` interfaces together. On the FortiGate-50B only one interface is configured as the default heartbeat interface. To change the heartbeat interface configuration, enter a list of interface name and priority pairs. Enter the name of each interface followed by the priority. Use a space to separate each interface name and priority pair. If you want to remove an interface from the list, add an interface to the list, or change a priority, you must retype the entire updated list. Heartbeat communication must be enabled on at least one interface. If heartbeat communication is interrupted the cluster stops processing traffic. You can select up to 8 heartbeat interfaces. This limit only applies to FortiGate units with more than 8 physical interfaces.	Depends on the FortiGate model.
`helo-holddown <holddown_integer>`	The hello state hold-down time, which is the number of seconds that a cluster unit waits before changing from hello state to work state. A cluster unit changes from hello state to work state when it starts up. The hello state hold-down time range is 5 to 300 seconds.	`20`

Variable	Description	Default
`link-failed-signal {disable | enable}`	Enable or disable shutting down all primary unit interfaces (except for heartbeat device interfaces) for one second when a link failover occurs. If all interfaces are not shut down in this way, some switches may not detect that the primary unit has become a subordinate unit and may keep sending packets to the former primary unit.	`disable`
`load-balance-all {disable | enable}`	If `mode` is set to `a-a`, configure active-active HA to load balance TCP sessions and sessions for firewall policies that include protection profiles or to just load balance sessions for firewall policies that include protection profiles. Enter `enable` to load balance TCP sessions and sessions for firewall policies that include protection profiles. Enter `disable` to load balance only sessions for firewall policies that include protection profiles. UDP, ICMP, multicast, and broadcast traffic is never load balanced and is always processed by the primary unit. VoIP traffic, IM traffic, IPSec VPN traffic, and SSL VPN traffic is also always processed only by the primary unit.	`disable`
`mode {a-a | a-p | standalone}`	Set the HA mode. Enter `a-p` to create an Active-Passive HA cluster, in which the primary cluster unit is actively processing all connections and the other cluster units are passively monitoring the cluster status and remaining synchronized with the primary cluster unit. Enter `a-a` to create an Active-Active HA cluster, in which each cluster unit is actively processing connections and monitoring the status of the other FortiGate units. All members of an HA cluster must be set to the same HA mode. Not available if a FortiGate interface `mode` is set to `dhcp` or `pppoe`. `a-a` mode is not available for virtual clusters.	`standalone`
`monitor <interface_names>`	Enable or disable port monitoring for link failure. Port monitoring (also called interface monitoring) monitors FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks. Enter the names of the interfaces to monitor. Use a space to separate each interface name. If you want to remove an interface from the list or add an interface to the list you must retype the list with the names changed as required. You can monitor physical interfaces, redundant interfaces, and 802.3ad aggregated interfaces but not VLAN subinterfaces or IPSec VPN interfaces. You cannot monitor interfaces that are 4-port switches. This includes the internal interface of FortiGate models 50B, 60, 60M, 100A, 200A, and FortiWiFi-60. This also includes the LAN interface of the FortiGate-500A. You can monitor up to 16 interfaces. This limit only applies to FortiGate units with more than 16 physical interfaces.	No default
`override {disable | enable}`	Enable or disable forcing the cluster to renegotiate and select a new primary unit every time a cluster unit leaves or joins a cluster, changes status within a cluster, or every time the HA configuration of a cluster unit changes. The override setting is not synchronized to all cluster units. Enabling override makes cluster operation more predictable but may lead to the cluster negotiating more often. During cluster negotiation traffic may be interrupted. For a virtual cluster configuration, override is enabled by default for both virtual clusters when you enter `set vcluster2 enable` to enable virtual cluster 2. Usually you would enable virtual cluster 2 and expect one cluster unit to be the primary unit for virtual cluster 1 and the other cluster unit to be the primary unit for virtual cluster 2. For this distribution to occur `override` must be enabled for both virtual clusters. Otherwise you will need to restart the cluster to force it to renegotiate. You can choose to disable `override` for both virtual clusters once the cluster is operating.	`disable` `enable` when you use `set vcluster2 enable` to enable virtual cluster 2.

Variable	Description	Default
password <password_str>	Enter a password for the HA cluster. The password must be the same for all FortiGate units in the cluster. The maximum password length is 15 characters. If you have more than one FortiGate HA cluster on the same network, each cluster must have a different password.	No default
pingserver-failover-threshold <threshold_integer>	Set the HA remote IP monitoring failover threshold. If HA remote monitoring is enabled using the pingserver-monitor-interface set the failover threshold so that if one or more ping servers fails, cluster failover occurs when the priority of all failed ping servers reaches or exceeds this threshold. You set the priority for each remote IP monitoring ping server using the ha-priority field of the command "system interface" on page 448. The failover threshold range is 0 to 50. Setting the failover threshold to 0 means that if any ping server added to the HA remote IP monitoring configuration fails an HA failover will occur.	0
pingserver-flip-timeout <timeout_integer>	Set the HA remote IP monitoring flip timeout in minutes. If HA remote IP monitoring fails on all cluster units because none of the cluster units can connect to the monitored IP addresses, the flip timeout stops a failover from occurring until the timer runs out. The range is 20 to 2147483647 minutes. For example, setting the pingserver-flip-timeout to 120 means that remote IP monitoring can only cause a failover every 120 minutes.	60
pingserver-monitor-interface <interface_names>	Enable HA remote IP monitoring by specifying the FortiGate unit interfaces that will be used to monitor remote IP addresses. You can configure remote IP monitoring for all types of interfaces including physical interfaces, VLAN interfaces, redundant interfaces and aggregate interfaces. Use a space to separate each interface name. If you want to remove an interface from the list or add an interface to the list you must retype the list with the names changed as required. For remote IP monitoring to work you must also: • Add ping servers to these interfaces. You can use the detectserver field of the command "system interface" on page 448 or you can add ping servers from the web-based manager. • Set the ha-priority field of the command "system interface" on page 448 for each ping server. • Set the pingserver-failover-threshold and pingserver-flip-timeout fields. For more information about configuring HA remote IP monitoring, see "Remote IP Monitoring Example" on page 444.	
priority <priority_integer>	Change the device priority of the cluster unit. Each cluster unit can have a different device priority (the device priority is not synchronized among cluster members). During HA negotiation, the cluster unit with the highest device priority becomes the primary unit. The device priority range is 0 to 255.	128
route-hold <hold_integer>	The time that the primary unit waits between sending routing table updates to subordinate units in a cluster. The route hold range is 0 to 3600 seconds.	10
route-ttl <ttl_integer>	The time to live for routes in a cluster unit routing table. The time to live range is 0 to 3600 seconds. The time to live controls how long routes remain active in a cluster unit routing table after the cluster unit becomes a primary unit. To maintain communication sessions after a cluster unit becomes a primary unit, routes remain active in the routing table for the route time to live while the new primary unit acquires new routes.	10

Variable	Description	Default
`route-wait <wait_integer>`	The time the primary unit waits after receiving a routing table update before sending the update to the subordinate units in the cluster. For quick routing table updates to occur, set `route-wait` to a relatively short time so that the primary unit does not hold routing table changes for too long before updating the subordinate units. The `route-wait` range is 0 to 3600 seconds.	0
`schedule {hub | ip | ipport | leastconnection | none | random | round-robin | weight-round-robin}`	Active-active load balancing schedule. **`hub`** — load balancing if the cluster interfaces are connected to hubs. Traffic is distributed to cluster units based on the Source IP and Destination IP of the packet. **`ip`** — load balancing according to IP address. If the cluster units are connected using switches, use `ip` to distribute traffic to units in a cluster based on the Source IP and Destination IP of the packet. **`ipport`** — load balancing according to IP address and port. If the cluster units are connected using switches, use `ipport` to distribute traffic to units in a cluster based on the source IP, source port, destination IP, and destination port of the packet. **`leastconnection`** — least connection load balancing. If the cluster units are connected using switches, use `leastconnection` to distribute traffic to the cluster unit currently processing the fewest connections. **`none`** — no load balancing. Use `none` when the cluster interfaces are connected to load balancing switches. **`random`** — random load balancing. If the cluster units are connected using switches, use `random` to randomly distribute traffic to cluster units. `round-robin` — round robin load balancing. If the cluster units are connected using switches, use `round-robin` to distribute traffic to the next available cluster unit. **`weight-round-robin`** — weighted round robin load balancing. Similar to round robin, but you can use the `weight` field to assign weighted values to each of the units in a cluster based on their capacity and on how many connections they are currently processing. For example, the primary unit should have a lower weighted value because it handles scheduling and forwards traffic. Weighted round robin distributes traffic more evenly because units that are not processing traffic are more likely to receive new connections than units that are very busy. You can optionally use the `weight` field to set a weighting for each cluster unit.	`round-robin`
`session-pickup {disable | enable}`	Enable or disable session pickup. Enable `session-pickup` so that if the primary unit fails, all sessions are picked up by the new primary unit. If you enable session pickup the subordinate units maintain session tables that match the primary unit session table. If the primary unit fails, the new primary unit can maintain all active communication sessions. If you do not enable session pickup the subordinate units do not maintain session tables. If the primary unit fails all sessions are interrupted and must be restarted when the new primary unit is operating. You must enable session pickup for effective failover protection. If you do not require effective failover protection, leaving session pickup disabled may reduce HA CPU usage and reduce HA heartbeat network bandwidth usage.	`disable`
`sync-config {disable | enable}`	Enable or disable automatic synchronization of primary unit configuration changes to all cluster units.	`enable`

Variable	Description	Default
uninterruptable-upgrade {disable | enable}	Enable or disable upgrading the cluster without interrupting cluster traffic processing. If uninterruptable-upgrade is enabled, traffic processing is not interrupted during a normal firmware upgrade. This process can take some time and may reduce the capacity of the cluster for a short time. If uninterruptable-upgrade is disabled, traffic processing is interrupted during a normal firmware upgrade (similar to upgrading the firmware operating on a standalone FortiGate unit).	enable

weight <priority_integer> <weight_integer>	The weighted round robin load balancing weight to assign to each cluster unit. When you set schedule to weight-round-robin you can use the weight field to set the weight of each cluster unit. The weight is set according to the priority of the unit in the cluster. A FortiGate HA cluster can contain up to four FortiGate units so you can set up to four weights.
	The default weight of 1 1 1 1 means that the four units in the cluster all have the same weight of 1.
	priority_integer is a number from 0 to 31 that identifies the priority of the cluster unit.
	weight-integer is a number between 0 and 31 that is the weight assigned to the cluster units according to their priority in the cluster. Increase the weight to increase the number of connections processed by the cluster unit with that priority.
	You enter the weight for each unit separately. For example, if you have a cluster of 4 FortiGate units you can set the weights for each unit as follows:
	`set weight 1 5`
	`set weight 2 10`
	`set weight 3 15`
	`set weight 4 20`
		1 1 1 1

vdom <vdom_names>	Add virtual domains to virtual cluster 1 or virtual cluster 2. Virtual cluster 2 is also called the secondary virtual cluster. In the config system ha shell, use set vdom to add virtual domains to virtual cluster 1. Adding a virtual domain to virtual cluster 1 removes that virtual domain from virtual cluster 2. In the config secondary-vcluster shell, use set vdom to add virtual domains to virtual cluster 2. Adding a virtual domain to virtual cluster 2 removes it from virtual cluster 1. You can use vdom to add virtual domains to a virtual cluster in any combination. You can add virtual domains one at a time or you can add multiple virtual domains at a time. For example, entering set vdom domain_1 followed by set vdom domain_2 has the same result as entering set vdom domain_1 domain_2.	All virtual domains are added to virtual cluster 1.
vcluster2 {disable | enable}	Enable or disable virtual cluster 2. In the global virtual domain configuration, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use config secondary-cluster to configure virtual cluster 2. Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1. Enabling virtual cluster 2 enables override for virtual cluster 1 and virtual cluster 2.	disable
config secondary-vcluster	Configure virtual cluster 2. You must enable vcluster2. Then you can use config secondary-vcluster to set monitor, override, priority, and vdom for virtual cluster 2.	Same defaults as virtual cluster 1 except that the default value for override is enable.

Examples

This example shows how to configure a FortiGate unit for active-active HA operation. The example shows how to set up a basic HA configuration by setting the HA `mode`, changing the `group-name`, and entering a `password`. You would enter the exact same commands on every FortiGate unit in the cluster. In the example virtual domains are not enabled.

```
config system ha
  set mode a-a
  set group-name myname
  set password HApass
end
```

The following example shows how to configure a FortiGate unit with virtual domains enabled for active-passive HA operation. In the example, the FortiGate unit is configured with three virtual domains (domain_1, domain_2, and domain_3) in addition to the root virtual domain. The example shows how to set up a basic HA configuration similar to the previous example; except that the HA mode can only be set to `a-p`. In addition, the example shows how to enable `vcluster2` and how to add the virtual domains domain_2 and domain_3 to `vcluster2`.

```
config global
  config system ha
    set mode a-p
    set group-name myname
    set password HApass
    set vcluster2 enable
    config secondary-vcluster
      set vdom domain_2 domain_3
    end
  end
end
```

The following example shows how to change the device priority of the primary unit to 200 so that this cluster unit always becomes the primary unit. When you log into the cluster you are actually connecting to the primary unit. When you change the device priority of the primary unit this change only affects the primary unit because the device priority is not synchronized to all cluster units. After you enter the following commands the cluster renegotiates and may select a new primary unit.

```
config system ha
  set priority 200
end
```

The following example shows how to change the device priority of a subordinate unit to 255 so that this subordinate unit becomes the primary unit. This example involves connecting to the cluster CLI and using the `execute ha manage 0` command to connect to the highest priority subordinate unit. After you enter the following commands the cluster renegotiates and selects a new primary unit.

```
execute ha manage 0
  config system ha
    set priority 255
  end
```

The following example shows how to change the device priority of the primary unit in virtual cluster 2. The example involves connecting to the virtual cluster CLI and changing the global configuration. In the example virtual cluster 2 has already been enabled so all you have to do is use the `config secondary-vcluster` command to configure virtual cluster 2.

```
config global
  config system ha
    config secondary-vcluster
      set priority 50
```

```
    end
  end
end
```

The following example shows how to change the default heartbeat interface configuration so that the port4 and port1 interfaces can be used for HA heartbeat communication and to give the port4 interface the highest heartbeat priority so that port4 is the preferred HA heartbeat interface.

```
config system ha
  set hbdev port4 100 port1 50
end
```

The following example shows how to enable monitoring for the external, internal, and DMZ interfaces.

```
config system ha
  set monitor external internal dmz
end
```

The following example shows how to configure weighted round robin weights for a cluster of three FortiGate units. You can enter the following commands to configure the weight values for each unit:

Table 10: Example weights for three cluster units

Cluster unit priority	Weight
0	1
1	3
2	3

```
config system ha
  set schedule weight-round-robin
  set weight 0 1
  set weight 1 3
  set weight 2 3
end
```

These commands have the following results:

- The first connection is processed by the primary unit (priority 0, weight 1)
- The next three connections are processed by the first subordinate unit (priority 1, weight 3)
- The next three connections are processed by the second subordinate unit (priority 2, weight 3)

The subordinate units process more connections than the primary unit, and both subordinate units, on average, process the same number of connections.

This example shows how to display the settings for the `system ha` command.

```
get system ha
```

This example shows how to display the configuration for the `system ha` command.

```
show system ha
```

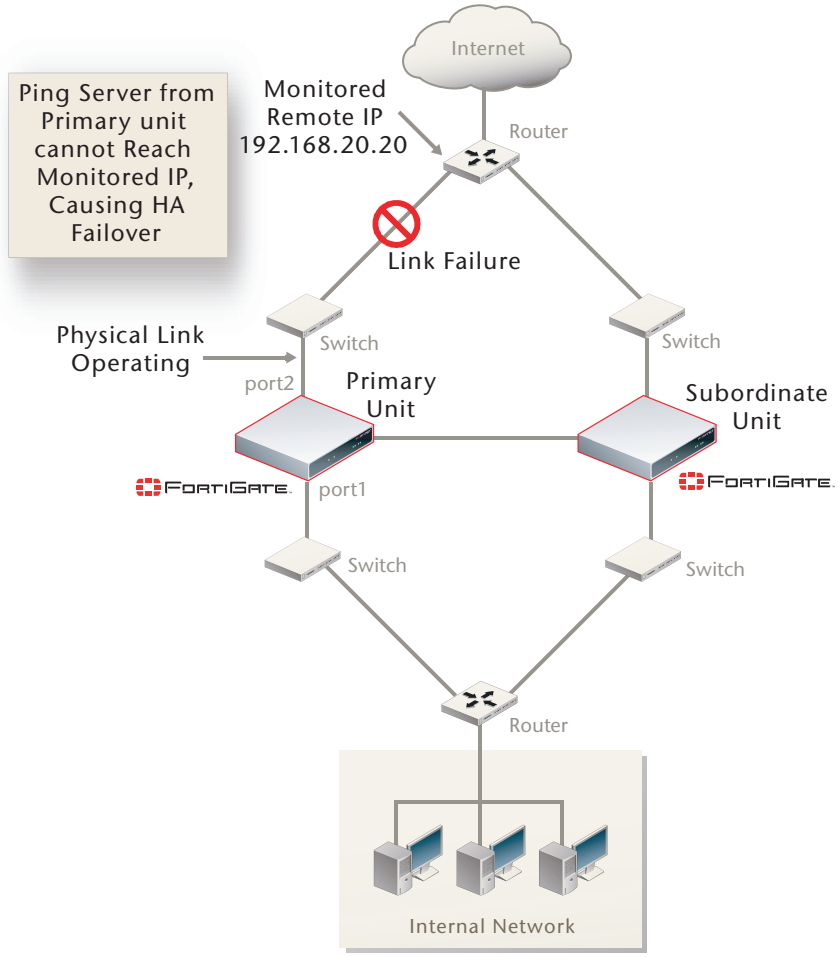
Remote IP Monitoring Example

HA Remote IP monitoring is similar to HA port monitoring. Port monitoring causes a cluster to failover if a monitored primary unit interface fails or is disconnected. Remote IP monitoring uses ping servers configured on FortiGate interfaces on the primary unit to test connectivity with IP addresses of network devices. Usually these would be IP addresses of network devices not directly connected to the cluster. Remote IP monitoring causes a failover if one or more of these remote IP addresses does not respond to a ping server.

Using remote IP monitoring to select a new primary unit can be useful in a number of ways depending on your network configuration. For example, in a full mesh HA configuration, with remote IP monitoring the cluster can detect failures in network equipment that is not directly connected to the cluster but that would interrupt traffic processed by the cluster if the equipment failed. In the example topology shown in Figure 5, the switch connected directly to the primary unit is operating normally but the link on the other side of the switches fails. As a result traffic can no longer flow between the primary unit and the Internet.

To detect this failure you can create a remote IP monitoring configuration consisting of a ping server on port2 of the cluster. The primary unit tests connectivity to 192.168.20.20. If the ping server cannot connect to 192.268.20.20 the cluster to fails over and the subordinate unit becomes the new primary unit. The remote HA monitoring ping server on the new primary unit can connect to 192.168.20.20 so the failover maintains connectivity between the internal network and the Internet through the cluster.

Figure 5: Example HA remote IP monitoring topology



To configure remote IP monitoring

1 Enter the following commands to configure HA remote monitoring for the example topology.

- Enter the `pingserver-monitor-interface` field to enable HA remote IP monitoring on port2.
- Enter the `pingserver-failover-threshold` field to set the HA remote IP monitoring failover threshold to 10. If one or more ping servers fails, cluster failover occurs when the priority of all failed ping servers reaches or exceeds this threshold. You set the priority for each ping server using the `ha-priority` field as described in step 2 below.
- Enter the `pingserver-flip-timeout` field to set the flip timeout to 120 minutes. After a failover, if HA remote IP monitoring on the new primary unit also causes a failover, the flip timeout prevents the failover from occurring until the timer runs out. Setting the `pingserver-flip-timeout` to 120 means that remote IP monitoring can only cause a failover every 120 minutes. This flip timeout is required to prevent repeating failovers if remote IP monitoring causes a failover from all cluster units because none of the cluster units can connect to the monitored IP addresses.

```
config system ha
  set pingserver-monitor-interface port2
  set pingserver-failover-threshold 10
  set pingserver-flip-timeout 120
end
```

2 Enter the following commands to add the ping server to the port2 interface and to set the HA remote IP monitoring priority for this ping server.

- Enter the `detectserver` field to add the ping server and set the ping server IP address to 192.168.20.20.
- Enter the `ha-priority` field to set the HA remote IP monitoring priority of the ping server to 10 so that if this ping server does not connect to 192.168.20.20 the HA remote IP monitoring priority will be high enough to reach the failover threshold and cause a failover.

```
config system interface
  edit port2
    set detectserver 192.168.20.20
    set ha-priority 10
  end
```

3 You can also use the `config global` command to change the time interval between ping server pings using the `interval` field and to change the number of times that the ping fails before a failure is detected using the `failtime` field.

4 You can also do the following to configure HA remote IP monitoring to test more IP addresses:

- Enable HA remote IP monitoring on more interfaces by adding more interface names to the `pingserver-monitor-interface` field.
- If your FortiGate configuration includes VLAN interfaces, aggregate interfaces and other interface types, you can add the names of these interfaces to the `pingserver-monitor-interface` field to configure HA remote IP monitoring for these interfaces.
- Add a second IP address to the `detectserver` field to monitor two IP addresses on each interface.

Note: If you add two IP addresses to the `detectserver` field the ping will be sent to both at the same time, and only when neither server responds will the ping server fail.

- Add secondary IPs to any interface and enter `detectserver` and `ha-priority` for each of the secondary IPs. You can do this to monitor multiple IP addresses on any interface and set a different HA priority for each one. By adding multiple ping servers to the remote HA monitoring configuration and setting the HA priorities for each you can fine tune remote IP monitoring. For example, if its more important to maintain connections to some remote IPs you can set the HA priorities higher for these IPs. And if its less important to maintain connections to other remote IPs you can set the HA priorities lower for these IPs. You can also adjust the `pingserver-failover-threshold` so that if the cluster cannot connect to one or two high priority IPs a failover occurs. But a failover will not occur if the cluster cannot connect to one or two low priority IPs.

Command History

FortiOS v2.80	Revised.
FortiOS v2.80 MR2	Added `load-balance-all` field.
FortiOS v2.80 MR5	Added `route-hold`, `route-wait`, and `route-ttl` fields.
FortiOS v2.80 MR6	Added `authentication`, `arps`, `encryption`, `hb-lost-threshold`, `helo-holddown`, and `hb-interval` fields.
FortiOS v2.80 MR7	Changes to the `weight` field.
FortiOS v2.80 MR10	New `link-failed-signal` field.
FortiOS v3.0	Added the `group-name`, `session-pickup`, `sync-config`, `vdom`, `vcluster2`, and `config secondary-vcluster` fields. The `monitor` and `hbdev` functionality has been simplified; priority numbers are no longer supported.
FortiOS v3.0 MR3	Added `uninterruptable-upgrade` field.
FortiOS v3.0 MR4	Priorities added back to the `hbdev` field.
FortiOS v3.0 MR5	In a virtual cluster configuration `override` is enabled for virtual cluster 1 and virtual cluster 2 when you enter `set vcluster2 enable` to enable virtual cluster 2.
FortiOS v3.0 MR6	Added the `arps-interval`, `pingserver-monitor-interface`, `pingserver-failover-threshold`, and `pingserver-flip-timeout` fields. Improved the description of the `arps` field.
FortiOS v3.0 MR7	The maximum length of the `group-name` increased from 7 to 32 characters.

interface

Use this command to edit the configuration of a FortiGate physical interface, VLAN subinterface, IEEE 802.3ad aggregate interface, redundant interface, or IPSec tunnel interface.

In the following table, VLAN subinterface can be substituted for interface in most places except that you can only configure VLAN subinterfaces with static IP addresses. Use the edit command to add a VLAN subinterface.

Note: VLAN communication over the backplane interfaces is available for FortiGate-5000 modules installed in a FortiGate-5020 chassis. The FortiSwitch-5003 does not support VLAN-tagged packets so VLAN communication is not available over the FortiGate-5050 and FortiGate-5140 chassis backplanes.

Some fields are specific to aggregate interfaces. These appear at the end of the list of commands under "variables for aggregate and redundant interfaces (models 300A, 310B, 400A, 500A, 620B, and 800 or higher)" on page 464.

Some FortiGate models support switch mode for the internal interfaces. Switch mode allows you to configure each interface on the switch separately with their own interfaces. A VLAN can not be configured on a switch interface. For more information, see "global" on page 423.

Using the one-arm intrusion detection system (IDS), you can now configure a FortiGate unit to operate as an IDS appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets. For more information, see the ips-sniffer-mode {enable | disable} field.

An interface's IPv6 address can be included in a Multi Listener Discovery (MLD) report. By default the FortiGate unit includes no addresses in the MLD report. For more information, see the ip6-send-adv {enable | disable} field.

Syntax

Entering a name string for the `edit` field that is not the name of a physical interface adds a VLAN subinterface.

```
config system interface
  edit <interface_name>
    set allowaccess <access_types>
    set alias <name_string>
    set arpforward {enable | disable}
    set auth-type <ppp_auth_method>
    set bfd {enable | disable | global}
    set bfd-desired-min-tx <interval_msec>
    set bfd-detect-mult <multiplier>
    set bfd-required-min-rx <interval_msec>
    set broadcast-forward {enable | disable}
    set ddns {enable | disable}
    set ddns-domain <ddns_domain_name>
    set ddns-password <ddns_password>
    set ddns-profile-id <dnsart_profile_id>
    set ddns-server <ddns_service>
    set ddns-sn <ddns_sn>
    set ddns-username <ddns_username>
    set defaultgw {enable | disable}
    set description <text>
    set detectprotocol <detection-protocols>
    set detectserver <pingserver_ipv4> [pingserver2_ipv4]
    set dhcp-client-identifier <client_name_str>
    set dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>}
```

```
set dhcp-relay-service {enable | disable}
set dhcp-relay-type {ipsec | regular}
set disc-retry-timeout <pppoe_retry_seconds>
set distance <admin_distance>
set dns-query {recursive | non-recursive | disable}
set dns-server-override {enable | disable}
set forward-domain <collision_group_number>
set fp-anomaly [...]
set gwdetect {enable | disable}
set ha-priority <priority_integer>
set icmp-redirect {enable | disable}
set ident-accept {enable | disable}
set idle-timeout <pppoe_timeout_seconds>
set inbandwidth <bandwidth_integer>
set interface <port_name>
set ip <interface_ipv4mask>
set ipmac {enable | disable}
set ips-sniffer-mode {enable | disable}
set ipunnumbered <unnumbered_ipv4>
set l2forward {enable | disable}
set l2tp-client {enable | disable}
set lacp-ha-slave {enable | disable}
set lacp-mode {active | passive | static}
set lacp-speed {fast | slow}
set lcp-echo-interval <lcp_interval_seconds>
set lcp-max-echo-fails <missed_echoes>
set log {enable | disable}
set macaddr <mac_address>
set mediatype {serdes-sfp | sgmii-sfp}
set member <if_name1> <if_name2> ...
set mode <interface_mode>
set mtu <mtu_bytes>
set mtu-override {enable | disable}
set netbios-forward {disable | enable}
set nontp-web-proxy {disable | enable}
set outbandwidth <bandwidth_integer>
set padt-retry-timeout <padt_retry_seconds>
set password <pppoe_password>
set peer-interface <interface>
set pppoe-unnumbered-negotiate {disable | enable}
set pptp-client {disable | enable}
set pptp-user <pptp_username>
set pptp-password <pptp_userpassword>
set pptp-server-ip <pptp_serverid>
set pptp-auth-type <pptp_authtype>
set pptp-timeout <pptp_idletimeout>
set priority <learned_priority>
set remote-ip <ipv4>
set speed <interface_speed>
set status {down | up}
set stpforward {enable | disable}
set subst {enable | disable}
set substitute-dst-mac <destination_mac_addres>
set tcp-mss <max_send_bytes>
```

```
set type {aggregate | hard-switch | hdlc | loopback | physical |
   redundant | tunnel | vap-switch | vdom-link | vlan | wireless}
set username <pppoe_username>
set vdom <vdom_name>
set vlanforward {enable | disable}
set vlanid <id_number>
set wccp {enable | disable}
set wifi-acl {allow | deny}
set wifi-auth {PSK | RADIUS}
set wifi-broadcast_ssid {enable | disable}
set wifi-encrypt {AES | TKIP}
set wifi-fragment_threshold <packet_size>
set wifi-key <hex_key>
set wifi-mac-filter {enable | disable}
set wifi-passphrase <pass_str>
set wifi-radius-server <server_name>
set wifi-rts_threshold <integer>
set wifi-security <sec_mode>
set wifi-ssid <id_str>
set wins-ip <wins_server_ip>
config ipv6
  set autoconf {enable | disable}
  set ip6-address <if_ipv6mask>
  set ip6-allowaccess <access_types>
  set ip6-default-life <ipv6_life_seconds>
  set ip6-hop-limit <ipv6_hops_limit>
  set ip6-link-mtu <ipv6_mtu>
  set ip6-manage-flag {disable | enable}
  set ip6-max-interval <adverts_max_seconds>
  set ip6-min-interval <adverts_min_seconds>
  set ip6-other-flag {disable | enable}
  set ip6-reachable-time <reachable_msecs>
  set ip6-retrans-time <retrans_msecs>
  set ip6-send-adv {enable | disable}
  config ip6-prefix-list
    edit <ipv6_prefix>
      set autonomous-flag {enable | disable}
      set onlink-flag {enable | disable}
      set preferred-life-time <seconds>
      set valid-life-time <seconds>
    end
  end
end
config l2tp-client-settings
  set auth-type {auto | chap | mschapv1 | mschapv2 | pap}
  set defaultgw {enable | disable}
  set distance <admin_distance>
  set mtu <integer>
  set password <password>
  set peer-host <ipv4_addr>
  set peer-mask <netmask>
  set peer-port <port_num>
  set priority <integer>
  set user <string>
```

```
end
config secondaryip
  edit <secondary_ip_id>
    set allowaccess <access_types>
    set detectserver <pingserver_ipv4> [pingserver2_ipv4]
    set gwdetect {enable | disable}
    set ha-priority <priority_integer>
    set ip <interface_ipv4mask>
  end
end
config wifi-mac_list
  edit <entry_number>
    set mac <mac_address>
  end
```

Note: A VLAN cannot have the same name as a zone or a virtual domain.

Variable	Description	Default
`allowaccess <access_types>`	Enter the types of management access permitted on this interface or secondary IP address. Valid types are: `http https ping snmp ssh telnet`. Separate each type with a space. To add or remove an option from the list, retype the complete list as required.	Varies for each interface.
`alias <name_string>`	Enter an alias name for the interface. Once configured, the alias will be displayed with the interface name to make it easier to distinguish. The alias can be a maximum of 25 characters. This option is only available when interface type is `physical`.	
`arpforward {enable | disable}`	Enable or disable forwarding of ARP packets on this interface. ARP forwarding is required for DHCP relay and MS Windows Client browsing.	`enable`
`auth-type <ppp_auth_method>`	Select the PPP authentication method for this interface. Choose one of: **`auto`** — select authentication method automatically **`chap`** — CHAP **`mschapv1`** — Microsoft CHAP v1 **`mschapv2`** — Microsoft CHAP v2 **`pap`** — PAP This is available only when `mode` is `pppoe`, and `type` of interface is `physical`.	auto
`bfd {enable | disable | global}`	The status of Bidirectional Forwarding Detection (bfd) on this interface: **`enable`** — enable BFD and ignore global BFD configuration. **`disable`** — disable BFD on this interface. **`global`** — BFD behavior on this interface will be based on the global configuration for BFD. The other bfd* fields are visible only if bfd is enabled.	`global`
`bfd-desired-min-tx <interval_msec>`	Enter the minimum desired interval for the BFD transmit interval. Valid range is from 1 to 100 000 msec.	50
`bfd-detect-mult <multiplier>`	Select the BFD detection multiplier.	3

Variable	Description	Default
bfd-required-min-rx <interval_msec>	Enter the minimum required interface for the BFD receive interval. Valid range is from 1 to 100 000 msec.	50
broadcast-forward {enable | disable}	Select to enable automatic forwarding of broadcast packets. Use with caution.	disable
ddns {enable | disable}	Enable to use a Dynamic DNS service (DDNS). If this interface of your FortiGate unit uses a dynamic IP address, you can arrange with a DDNS service provider to use a domain name to provide redirection of traffic to your network whenever the IP address changes. DDNS is only available in NAT/Route mode.	disable
ddns-domain <ddns_domain_name>	Enter the fully qualified domain name to use for the DDNS. This is the domain name you have registered with your DDNS. This variable is only available when ddns is enabled, but ddns-server is not set to dnsart.com.	No default.
ddns-password <ddns_password>	Enter the password to use when connecting to the DDNS server. This is only available when ddns is enabled, but ddns-server is not set to dipdns.net.	No default.
ddns-profile-id <dnsart_profile_id>	Enter your DDNS profile ID. This field replaces ddns-domain. This variable is only available when ddns is enabled, and ddns-server is set to dnsart.com.	No default.
ddns-server <ddns_service>	Select a DDNS server to use. The client software for these services is built into the FortiGate firmware. The FortiGate unit can only connect automatically to a DDNS server for these supported clients. **dhs.org** — supports members.dhs.org and dnsalias.com. **dipdns.net** — supports dipdnsserver.dipdns.com. **dnsart.com** — supports www.dnsart.com. **dyndns.org** — supports members.dyndns.org. **dyns.net** — supports www.dyns.net. **now.net.cn** — supports ip.todayisp.com. **ods.org** — supports ods.org. **tzo.com** — supports rh.tzo.com. **vavic.com** — supports ph001.oray.net. This variable is only available when ddns is enabled.	No default.
ddns-sn <ddns_sn>	Enter your DDNS serial number. This variable is only available if ddns is enabled, and ddns-server is set to dipdns.net. This field replaces ddns-username and ddns-password.	No default.
ddns-username <ddns_username>	Enter the user name to use when connecting to the DDNS server. This is available when ddns is enabled, but ddns-server is not set to dipdns.net.	No default.
defaultgw {enable | disable}	Enable to get the gateway IP address from the DHCP or PPPoE server. This is valid only when the mode is one of DHCP or PPPoE.	disable
description <text>	Optionally, enter up to 63 characters to describe this interface.	No default.
detectprotocol <detection-protocols>	Select the protocols to use to detect interface connection status. You can select: ping tcp-echo udp-echo. You can select multiple protocols by separating each protocol with a space.	ping

Variable	Description	Default
`detectserver <pingserver_ipv4> [pingserver2_ipv4]`	Add the IP address of a server to be detected by interface connection status. The server is usually the next hop router on the network connected to the interface. If `gwdetect` is enabled, the FortiGate unit confirms connectivity with the server at this IP address. Adding a detect server is required for routing failover. You can use the `detectprotocol` field to set the protocols used to detect the server. Optionally you can add 2 servers. The FortiGate unit will send to both at the same time, and only when neither server responds will `gwdetect` fail. A primary and secondary ping server IP address can be the same. This is available only in NAT/Route mode.	No default.
`dhcp-client-identifier <client_name_str>`	Override the default DHCP client identifier used by this interface.The DHCP client identifier is used by DHCP to identify individual DHCP clients (in this case individual FortiGate interfaces). By default the DHCP client identifier for each FortiGate interface is created based on the FortiGate model name and the interface MAC address. In some cases you may want to specify your own DHCP client identifier using this command. This is available if `mode` is set to `dhcp`.	
`dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>}`	Set DHCP relay IP addresses. You can specify up to eight DHCP relay servers for DHCP coverage of subnets. Replies from all DHCP servers are forwarded back to the client. The client responds to the offer it wants to accept. Do not set `dhcp-relay-ip` to 0.0.0.0.	No default.
`dhcp-relay-service {enable | disable}`	Enable to provide DHCP relay service on this interface. The DHCP type relayed depends on the setting of `dhcp-relay-type`. There must be no other DHCP server of the same type (regular or ipsec) configured on this interface.	`disable`
`dhcp-relay-type {ipsec | regular}`	Set `dhcp_type` to `ipsec` or `regular` depending on type of firewall traffic.	`regular`
`disc-retry-timeout <pppoe_retry_seconds>`	Set the initial PPPoE discovery timeout in seconds. This is the time to wait before retrying to start a PPPoE discovery. Set to 0 to disable this feature. This field is only available in NAT/Route mode when `mode` is set to `pppoe`.	1
`distance <admin_distance>`	Configure the administrative distance for routes learned through PPPoE or DHCP. Use the administrative distance to specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. Distance can be an integer from 1-255. For more information, see router static "distance <distance>" on page 361 This variable is only available in NAT/Route mode when `mode` is set to `dhcp` or `pppoe`.	1
`dns-query {recursive | non-recursive | disable}`	Configure the interface to accept DNS queries. **`disable`** — Disable accepting DNS queries. **`non-recursive`** — Look up domain name in local database. Do not relay the request to the DNS server configured for the FortiGate unit. See "system dns-database" on page 414. **`recursive`** — Look up domain name in local database. If the entry is not found, relay the request to the DNS server configured for the FortiGate unit.	`disable` On models 100 and lower, the Internal interface defaults to `recursive`.
`dns-server-override {enable | disable}`	Disable to prevent this interface from using DNS server addresses it acquires via DHCP or PPPoe. This variable is only displayed if `mode` is set to `dhcp` or `pppoe`.	`enable`

Variable	Description	Default
`edit <interface_name>`	Edit an existing interface or create a new VLAN interface.	None.
`edit <ipv6_prefix>`	Enter the IPv6 prefix you want to configure. For settings, see the edit <ipv6_prefix> variables section of this table.	None.
`edit <secondary_ip_id>`	Enter an integer identifier, e.g., 1, for the secondary ip address that you want to configure.	None.
`explicit-web-proxy {enable | disable}`	Enable explicit Web proxy on this interface. For more information, see "explicit" on page 656.	`disable`
`forward-domain <collision_group_number>`	Specify the collision domain to which this interface belongs. Layer 2 broadcasts are limited to the same group. By default, all interfaces are in group 0. Collision domains prevent the forwarding of ARP packets to all VLANs on an interface. Without collision domains, duplicate MAC addresses on VLANs may cause ARP packets to be duplicated. Duplicate ARP packets can cause some switches to reset. This command is only available in Transparent mode. For more information see "Working with virtual domains" on page 53 or *FortiGate VLANs and VDOMs*.	`0`
`fp-anomaly [...]`	Enable NP2 hardware fast path anomaly checking on an interface and specify whether to drop or allow (pass) different types of anomalies. When no options are specified, anomaly checking performed by the network processor is disabled. If pass options are specified, packets may still be rejected by other anomaly checks, including policy-required IPS performed using the FortiGate unit main processing resources. Log messages are generated when packets are dropped due to options in this setting. The fp-anomaly option is available for NP2-enabled interfaces. For more information, see the Fortinet Hardware Acceleration Technical Note.	`No options specified (disabled)`
`gwdetect {enable | disable}`	Enable or disable confirming connectivity with the server at the `detectserver` IP address using the configured `detectprotocol` protocols. The frequency with which the FortiGate unit confirms connectivity is set using the `failtime` and `interval` fields in the command "system global" on page 423.	`disable`
`ha-priority <priority_integer>`	The HA priority to assign to the ping servers configured on an interface when the interface is added to an HA remote IP monitoring configuration. The priority range is 0 to 50. You configure HA remote IP monitoring using the `pingserver-monitor-interface` field in the command "system ha" on page 435. You can set `ha-priority` for all types of interfaces including physical interfaces, VLAN interfaces, and secondary IPs. This field is not available in Transparent mode.	0
`icmp-redirect {enable | disable}`	Disable to stop ICMP redirect from sending from this interface. ICMP redirect messages are sent by a router to notify the original sender of packets that there is a better route available.	`enable`
`ident-accept {enable | disable}`	Enable or disable passing ident packets (TCP port 113) to the firewall policy. If set to disable, the FortiGate unit sends a TCP reset packet in response to an ident packet.	`disable`
`idle-timeout <pppoe_timeout_seconds>`	Disconnect if the PPPoE connection is idle for the specified number of seconds. Set to zero to disable this feature. This is available when `mode` is set to `pppoe`.	0

Variable	Description	Default
inbandwidth <bandwidth_integer>	Enter the KB/sec limit for incoming traffic for this interface. Use this command to configure inbound traffic shaping for an interface. Inbound traffic shaping limits the bandwidth accepted by the interface. Limiting inbound traffic takes precedence over traffic shaping applied by firewall policies. You can set inbound traffic shaping for any FortiGate unit interface and it can be active for more than one FortiGate unit interface at a time. Setting <bandwidth_integer> to 0 (the default) means unlimited bandwidth or no traffic shaping.	0
interface <port_name>	Enter the physical interface this virtual interface is linked to. This is available only when adding virtual interfaces such as VLANs and VPNs.	None.
ip <interface_ipv4mask>	Enter the interface IP address and netmask. This is not available if mode is set to dhcp or pppoe. You can set the IP and netmask, but it will not display. This is only available in NAT/Route mode. The IP address cannot be on the same subnet as any other FortiGate unit interface.	Varies for each interface.
ipmac {enable | disable}	Enable or disable IP/MAC binding for the specified interface. For information about configuring IP/MAC binding settings, see “ipmacbinding setting” on page 119 and “ipmacbinding table” on page 121.	disable
ips-sniffer-mode {enable | disable}	Enable to configure this interface to operate as a one-armed sniffer as part of configuring a FortiGate unit to operate as an IDS appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets. Once the interface is enabled for sniffing you cannot use the interface for other traffic. You must add sniffer policies for the interface to actually sniff packets. For more information on one-armed IPS, see “firewall sniff-interface-policy” on page 182 and “firewall sniff-interface-policy6” on page 185.	disable
ipunnumbered <unnumbered_ipv4>	Enable IP unnumbered mode for PPPoE. Specify the IP address to be borrowed by the interface. This IP address can be the same as the IP address of another interface or can be any IP address. This is only available when mode is pppoe. The Unnumbered IP may be used for PPPoE interfaces for which no unique local address is provided. If you have been assigned a block of IP addresses by your ISP for example, you can add any of these IP addresses to the Unnumbered IP.	No default.
l2forward {enable | disable}	Enable to allow layer-2 forwarding for this interface. If there are layer-2 protocols such as IPX, PPTP or L2TP in use on your network, you need to configure your FortiGate unit interfaces to pass these protocols without blocking. Enabling l2forward may cause packets to repeatedly loop through the network, much like a broadcast storm. In this case either disable l2forward, or enable Spanning Tree Protocol (STP) on your network’s switches and routers. For more information, see *FortiGate VLANs and VDOMs*.	disable
l2tp-client {enable | disable}	Enable or disable this interface as a Layer 2 Tunneling Protocol (L2TP) client. Enabling makes config l2tp-client-settings visible. You may need to enable l2forward on this interface. This is available only on FortiGate 50 series, 60 series, and 100A. The interface can not be part of an aggregate interface, and the FortiGate unit can not be in Transparent mode, or HA mode. If l2tp-client is enabled on an interface, the FortiGate unit will not enter HA mode until the L2TP client is disabled.	disable

Variable	Description	Default
`lcp-echo-interval <lcp_interval_seconds>`	Set the interval in seconds between PPPoE Link Control Protocol (LCP) echo requests. This is available only when `mode` is `pppoe`.	5
`lcp-max-echo-fails <missed_echoes>`	Set the maximum number of missed LCP echoes before the PPPoE link is disconnected. This is only available when `mode` is `pppoe`.	3
`log {enable | disable}`	Enable or disable traffic logging of connections to this interface. Traffic will be logged only when it is on an administrative port. All other traffic will not be logged. Enabling this setting may reduce system performance, and is normally used only for troubleshooting.	`disable`
`macaddr <mac_address>`	Override the factory set MAC address of this interface by specifying a new MAC address. Use the form xx:xx:xx:xx:xx:xx. Typically this is only used for virtual interfaces.	Factory set.
`mediatype {serdes-sfp | sgmii-sfp}`	Some FortiGate SFP interfaces can operate in SerDes (Serializer/Deserializer) or SGMII (Serial Gigabit Media Independent Interface) mode. The mode that the interface operates in depends on the type of SFP transceiver installed. Use this field to switch the interface between these two modes. Set `mediatype` to: **`serdes-sfp`** if you have installed a SerDes transceiver. In SerDes mode an SFP interface can only operate at 1000 Mbps. **`sgmii-sfp`** if you have installed an SGMII transceiver. In SGMII mode the interface can operate at 10, 100, or 1000 Mbps. This field is available for some FortiGate SFP interfaces. For example, all FortiGate-ASM-FB4 interfaces and interfaces port3 to port18 of the FortiGate-3016B support both SerDes and SGMII mode. See your FortiGate unit install guide for more information about what modes your FortiGate interfaces support.	`serdes-sfp`
`mode <interface_mode>`	Configure the connection mode for the interface as one of: **`static`** — configure a static IP address for the interface. **`dhcp`** — configure the interface to receive its IP address from an external DHCP server. **`pppoe`** — configure the interface to receive its IP address from an external PPPoE server. This is available only in NAT/Route mode. **`eoa`** — Ethernet over ATM **`ipoa`** — IP over ATM (also known as bridged mode). This variable is only available in NAT/Route mode.	`static`

Variable	Description	Default
`mtu <mtu_bytes>`	Set a custom maximum transmission unit (MTU) size in bytes. Ideally set `mtu` to the size of the smallest MTU of all the networks between this FortiGate unit and the packet destination. `<mtu_bytes>` valid ranges are: • 68 to 1 500 bytes in `static` mode • 576 to 1 500 bytes in `dhcp` mode • 576 to 1 492 bytes in `pppoe` mode • up to 9 000 bytes for NP2-accelerated interfaces • over 1 500 bytes on high end FortiGate models on some interfaces. If you enter an MTU that is not supported, an error message informs you of the valid range for this interface. In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces to match the new MTU. If you configure an MTU size larger than 1 500 on your FortiGate unit, all other network equipment on the route to the destination must also support that frame size. You can only set the MTU of a physical interface. All virtual interfaces will inherit that MTU from the physical parent interface. The variable `mtu` is only available when `mtu-override` is enabled.	1 500
`mtu-override {enable | disable}`	Select enable to use custom MTU size instead of default (1 500). This is available for physical interfaces only. If you change the MTU size, you must reboot the FortiGate unit to update the MTU values of the VLANs on this interface. FortiGate models 3000 and larger support MTU sizes larger than the standard 1 500 bytes.	`disable`
`netbios-forward {disable | enable}`	Enable to forward Network Basic Input/Output System (NetBIOS) broadcasts to a Windows Internet Name Service (WINS) server. Use wins-ip <wins_server_ip> to set the WINS server IP address. This variable is only available in NAT/Route mode.	`disable`
`nontp-web-proxy {disable | enable}`	Enable to turn on web cache support for this interface, such as accepting HTTP proxies and DNS requests. Web caching accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. For more information, see "web-proxy explicit" on page 656. This variable is only available when this interface is in NAT/Route mode. It is available on all models.	`disable`
`outbandwidth <bandwidth_integer>`	Enter the KB/sec limit for outgoing (egress) traffic for this interface. Use this command to configure outbound traffic shaping for an interface. Outbound traffic shaping limits the bandwidth accepted by the interface. Limiting outbound traffic takes precedence over traffic shaping applied by firewall policies. You can set outbound traffic shaping for any FortiGate interface and it can be active for more than one FortiGate interface at a time. Setting `<bandwidth_integer>` to 0 (the default) means unlimited bandwidth or no traffic shaping.	0
`padt-retry-timeout <padt_retry_seconds>`	Initial PPPoE Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP. This is available in NAT/Route mode when `mode` is `pppoe`.	1
`password <pppoe_password>`	Enter the password to connect to the PPPoE server. This is available in NAT/Route mode when `mode` is `pppoe`.	No default.

Variable	Description	Default
peer-interface <interface>	Select an interface to be used in TP mode, when the FortiGate unit cannot find the destination MAC address in the local table. This can happen during IPS test. The peer-interface cannot be the same interface, but it must be in the same VDOM. This option is only available in Transparent mode.	
pppoe-unnumbered-negotiate {disable | enable}	Disable to resolve problems when mode is set to PPPoE, and ipunnumbered is set. The default configuration may not work in some regions, such as Japan. This is only available when mode is pppoe and ipunnumbered is set.	enable
pptp-client {disable | enable}	Enable to configure and use a point-to-point tunneling protocol (PPTP) client. You may need to enable l2forward on this interface. This command is not available when in HA mode. If the pptp-client is enabled on an interface, the FortiGate unit will not enter HA mode until that pptp-client is disabled.	disable
pptp-user <pptp_username>	Enter the name of the PPTP user.	No default.
pptp-password <pptp_userpassword>	Enter the password for the PPTP user.	No default.
pptp-server-ip <pptp_serverid>	Enter the IP address for the PPTP server.	No default.
pptp-auth-type <pptp_authtype>	Enter the authentication type for the PPTP user.	No default.
pptp-timeout <pptp_idletimeout>	Enter the idle timeout in minutes. Use this timeout to shut down the PPTP user session if it is idle for this number of seconds. 0 for disabled.	No default.
priority <learned_priority>	Enter the priority of routes using this interface. For more information on priority, see “router static” on page 361. This is only available when mode is pppoe or dhcp.	No default.
remote-ip <ipv4>	Enter an IP address for the remote end of a tunnel interface. If you want to use dynamic routing with the tunnel, or be able to ping the tunnel interface, you must specify an address for the remote end of the tunnel in remote-ip and an address for this end of the tunnel in ip. This is only available if type is tunnel.	No default.
speed <interface_speed>	The interface speed: **auto** — the default speed. The interface uses auto-negotiation to determine the connection speed. Change the speed only if the interface is connected to a device that does not support auto-negotiation. **10full** — 10 Mbps, full duplex **10half** — 10 Mbps, half duplex **100full** — 100 Mbps, full duplex **100half** — 100 Mbps, half duplex **1000full** — 1000 Mbps, full duplex **1000half** — 1000 Mbps, half duplex Speed options vary for different models and interfaces. Enter a space and a “?” after the speed field to display a list of speeds available for your model and interface. You cannot change the speed for interfaces that are 4-port switches. This includes the internal interfaces of FortiGate models 60, 60M, 100A, 200A, and FortiWiFi-60. This also includes the LAN interface of the FortiGate-500A.	auto

Variable	Description	Default
spillover-threshold <threshold_int>	Set the spillover-threshold to limit the amount of bandwidth processed by the Interface. The range is 0-2097000 KBps. Set the spillover-threshold for an interface if the ECMP route failover and load balance method, configured by the v4-ecmp-mode field of the config system settings command is set to usage-based. The FortiGate unit sends all ECMP-routed sessions to the lowest numbered interface until the bandwidth being processed by this interface reaches its spillover threshold. The FortiGate unit then spills additional sessions over to the next lowest numbered interface.	0
status {down | up}	Start or stop the interface. If the interface is stopped, it does not accept or send packets. If you stop a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.	up (down for VLANs)
stpforward {enable | disable}	Enable to forward Spanning Tree Protocol (STP) packets through this interface. STP maps the network to provide the least-cost-path from point to point while blocking all other ports for that path. This prevents any loops which would flood the network. If your network uses layer-2 protocols, and has looping issues STP will stop this. For more information, see *FortiGate VLANs and VDOMs*.	disable
subst {enable | disable}	Enable to use a substitute destination MAC address for this address. This feature may be used with virtual interfaces to prevent network loops.	disable
substitute-dst-mac <destination_mac_addres>	Enter the substitute destination MAC address to use when subst is enabled. Use the xx:xx:xx:xx:xx:xx format.	No default.
tcp-mss <max_send_bytes>	Enter the FortiGate unit's maximum sending size for TCP packets.	No default.

Variable	Description	Default
`type {aggregate | hard-switch | hdlc | loopback | physical | redundant | tunnel | vap-switch | vdom-link | vlan | wireless}`	Enter the type of interface. Note: Some types are read only, and are set automatically by hardware. **`aggregate`** — available only on FortiGate models 800 and higher. Aggregate links use the 802.3ad standard to group up to 8 interfaces together. For aggregate specific fields, see "variables for aggregate and redundant interfaces (models 300A, 310B, 400A, 500A, 620B, and 800 or higher)" on page 464. **`hard-switch`** — used when a switch-interface is configured and unit electronics provides switch functionality. The switch-interface `type` field must be set to `switch-hardware`. For more information see "switch-interface" on page 530. **`hdlc`** — High-level Data Link Control (HDLC) is a bit-oriented synchronous data link layer protocol; it operates at Layer-2 of OSI model. It is an interface that supports T1/E1 connections. This type of interface is supported by some AMC cards. **`loopback`** — a virtual interface that is always up. This interface's status and link status are not affected by external changes. It is primarily used for blackhole routing - dropping all packets that match this route. This route is advertised to neighbors through dynamic routing protocols as any other static route. loopback interfaces have no dhcp settings, no forwarding, no mode, or dns settings. You can create a loopback interface from the CLI or web-based manager. **`physical`** — for reference only. All physical FortiGate interfaces and only these interfaces have `type` set to `physical` and the type cannot be changed. **`redundant`** — used to group 2 or more interfaces together for reliability. Only one interface is in use at any given time. If the first interface fails, traffic continues uninterrupted as it switches to the next interface in the group. This is useful in HA configurations. The order interfaces become active in the group is determined by the order you specify using the `set member` field. `tunnel` is for reference only - you cannot create tunnel interfaces using this command. Create GRE tunnels using the system gre-tunnel command. Create IPSec tunnels using the `vpn ipsec-intf phase1` command. **`vap-switch`** — for a wireless controller virtual access point (VAP). This type of interface is created automatically when you configure a VAP. **`vdom-link`** — an internal point-to-point interface object. This interface object is a link used to join virtual domains. For more information on vdom-links, see "vdom-link" on page 533. **`vlan`** — a virtual LAN interface. This is the type of interface created by default on any existing physical interface. VLANs increase the number of network interfaces beyond the physical connections on the unit. VLANs cannot be configured on a switch mode interface in Transparent mode. **`wireless`** — applies only to FortiWiFi-60A, -60AM, and -60B models.	`vlan` for newly created interface, `physical` otherwise.
`username <pppoe_username>`	Enter the user name used to connect to the PPPoE server. This is only available in NAT/Route mode when `mode` is set to `pppoe`.	No default.
`vdom <vdom_name>`	Enter the name of the virtual domain to which this interface belongs. When you change this field, the physical interface moves to the specified virtual domain. Virtual IP previously added for this interface are deleted. You should also manually delete any routes that include this interface as they may now be inaccessible. For more about VDOMs, see "Working with virtual domains" on page 53, and the FortiGate VLANs and VDOMs Guide.	`root`

Variable	Description	Default
`vlanforward {enable | disable}`	Enable or disable forwarding of traffic between VLANs on this interface. When disabled, all VLAN traffic will only be delivered to that VLAN only.	`enable`
`vlanid <id_number>`	Enter a VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface. The VLAN ID can be any number between 1 and 4094, as 0 and 4095 are reserved, but it must match the VLAN ID added by the IEEE 802.1Q-compliant router on the other end of the connection. Two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN ID to different physical interfaces, and you can add more multiple VLANs with different VLAN IDs to the same physical interface. This is available only when editing an interface with a type of `VLAN`. For more about VLANs, see the FortiGate VLANs and VDOMs Guide.	No default.
`wccp {enable | disable}`	Enable to start the Web Cache Control Protocol (WCCP) on this interface to optimize web traffic to reduce transmission costs and downloading time.	`disable`
`wins-ip <wins_server_ip>`	Enter the IP address of a WINS server to which to forward NetBIOS broadcasts. This WINS server address is only used if `netbios-forward` is enabled. This variable is only available in NAT/Route mode.	No default.
WiFi fields	These fields apply only to the FortiWiFi-60A and FortiWiFi-60AM unit when `type` is `wireless`.	
`mac <mac_address>`	Enter a MAC address for the MAC filter list. This is used in the `config wifi-mac_list` subcommand.	No default.
`wifi-acl {allow | deny}`	Select whether MAC filter list allows or denies access.	`deny`
`wifi-auth {PSK | RADIUS}`	Select either Pre-shared Key (PSK) or RADIUS to authenticate users connecting to this interface. This is available only when `wifi-security` is set to WPA.	`PSK`
`wifi-broadcast_ssid {enable | disable}`	Enable if you want FortiWiFi-60 to broadcast its SSID.	`disable`
`wifi-encrypt {AES | TKIP}`	Select either Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) for encryption on this WLAN interface. This is available only when `wifi-security` is set to WPA.	`TKIP`
`wifi-fragment_threshold <packet_size>`	Set the maximum size of a data packet before it is broken into smaller packets, reducing the chance of packet collisions. If the packet size is larger than the threshold, the FortiWiFi unit will fragment the transmission. If the packet size less than the threshold, the FortiWiFi unit will not fragment the transmission. Range 800-2346. A setting of 2346 bytes effectively disables this option. This is available in AP mode only.	`2346`
`wifi-key <hex_key>`	Enter a WEP key. The WEP key must be 10 or 26 hexadecimal digits (0-9 a-f). For a 64-bit WEP key, enter 10 hexadecimal digits. For a 128-bit WEP key, enter 26 hexadecimal digits. `wifi-security` must be set to `WEP128` or `WEP64`. This is available in AP mode only.	No default.
`wifi-mac-filter {enable | disable}`	Enable MAC filtering for the wireless interface.	`disable`

Variable	Description	Default
wifi-passphrase <pass_str>	Enter shared key for WPA_PSK security. wifi-security must be set to WPA_PSK. This is available in AP mode only.	No default.
wifi-radius-server <server_name>	Set RADIUS server name for WPA_RADIUS security. wifi-security must be set to WPA_RADIUS. This is available in AP mode only.	No default.
wifi-rts_threshold <integer>	The request to send (RTS) threshold is the maximum size, in bytes, of a packet that the FortiWiFi will accept without sending RTS/CTS packets to the sending wireless device. In some cases, larger packets being sent may cause collisions, slowing data transmissions. The valid range is 256 to 2346. A setting of 2347 bytes effectively disables this option. This is available in AP mode only.	2346
wifi-security <sec_mode>	Enter security (encryption) mode: **None** — Communication is not encrypted. **WEP64** — WEP 64-bit encryption **WEP128** — WEP 128-bit encryption **WPA_PSK** — WPA encryption with pre-shared key **WPA_RADIUS** — WPA encryption via RADIUS server. This is available in AP mode only.	None
wifi-ssid <id_str>	Change the Service Set ID (SSID) as required. The SSID is the wireless network name that this FortiWiFi-60A WLAN broadcasts. Users who wish to use the wireless network should configure their computers to connect to the network that broadcasts this network name.	fortinet
config ipv6 variables		
autoconf {enable | disable}	Enable or disable automatic configuration of the IPv6 address. When enabled, and ip6-send-adv is disabled, the FortiGate unit acts as a stateless address auto-configuration client (SLAAC).	disable
ip6-address <if_ipv6mask>	The interface IPv6 address and netmask. The format for IPv6 addresses and netmasks is described in RFC 3513. This is available in NAT/Route mode only.	::/0
ip6-allowaccess <access_types>	Enter the types of management access permitted on this IPv6 interface. Valid types are: ping or any. Both of these options only allow ping access.	Varies for each interface.
ip6-default-life <ipv6_life_seconds>	Enter the number, in seconds, to add to the Router Lifetime field of router advertisements sent from the interface. The valid range is 0 to 9000. This is available in NAT/Route mode only.	1800
ip6-hop-limit <ipv6_hops_limit>	Enter the number to be added to the Cur Hop Limit field in the router advertisements sent out this interface. Entering 0 means no hop limit is specified. This is available in NAT/Route mode only. This is available in NAT/Route mode only.	0
ip6-link-mtu <ipv6_mtu>	Enter the MTU number to add to the router advertisements options field. Entering 0 means that no MTU options are sent. This is available in NAT/Route mode only.	0
ip6-manage-flag {disable | enable}	Enable or disable the managed address configuration flag in router advertisements. This is available in NAT/Route mode only.	disable

Variable	Description	Default
ip6-max-interval <adverts_max_seconds>	Enter the maximum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface. The valid range is 4 to 1800. This is available in NAT/Route mode only.	600
ip6-min-interval <adverts_min_seconds>	Enter the minimum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface. The valid range is 4 to 1800. This is available in NAT/Route mode only.	198
ip6-other-flag {disable | enable}	Enable or disable the other stateful configuration flag in router advertisements. This is available in NAT/Route mode only.	disable
ip6-reachable-time <reachable_msecs>	Enter the number to be added to the reachable time field in the router advertisements. The valid range is 0 to 3600. Entering 0 means no reachable time is specified. This is available in NAT/Route mode only.	0
ip6-retrans-time <retrans_msecs>	Enter the number to be added to the Retrans Timer field in the router advertisements. Entering 0 means that the Retrans Timer is not specified. This is available in NAT/Route mode only.	0
ip6-send-adv {enable | disable}	Enable or disable the flag indicating whether or not to send periodic router advertisements and to respond to router solicitations. When enabled, this interface's address will be added to all-routers group (FF02::02) and be included in an Multi Listener Discovery (MLD) report. If no interfaces on the FortiGate unit have ip6-send-adv enabled, the FortiGate unit will only listen to the all-hosts group (FF02::01) which is explicitly excluded from MLD reports according to RFC 2710 section 5. When disabled, and autoconf is enabled, the FortiGate unit acts as a stateless address auto-configuration client (SLAAC). This is available in NAT/Route mode only.	disable
edit <ipv6_prefix> variables		
autonomous-flag {enable | disable}	Set the state of the autonomous flag for the IPv6 prefix.	disable
onlink-flag {enable | disable}	Set the state of the on-link flag ("L-bit") in the IPv6 prefix.	
preferred-life-time <seconds>	Enter the preferred lifetime, in seconds, for this IPv6 prefix.	604800
valid-life-time <seconds>	Enter the valid lifetime, in seconds, for this IPv6 prefix.	2592000
config l2tp-client-settings		
auth-type {auto | chap | mschapv1 | mschapv2 | pap}	Select the type of authorization used with this client: **auto** — automatically choose type of authorization. **chap** — use Challenge-Handshake Authentication Protocol. **mschapv1** — use Microsoft version of CHAP version 1. **mschapv2** — use Microsoft version of CHAP version 2. **pap** — use Password Authentication Protocol.	auto
defaultgw {enable | disable}	Enable to use the default gateway.	disable
distance <admin_distance>	Enter the administration distance of learned routes.	2
mtu <integer>	Enter the Maximum Transmission Unit (MTU) for L2TP.	1460
password <password>	Enter the password for L2TP.	n/a
peer-host <ipv4_addr>	Enter the IP address of the L2TP host.	n/a

Variable	Description	Default
`peer-mask <netmask>`	Enter the netmask used to connect to L2TP peers connected to this interface.	255.255.255.255
`peer-port <port_num>`	Enter the port used to connect to L2TP peers on this interface.	1701
`priority <integer>`	Enter the priority of routes learned through L2TP. This will be used to resolve any ties in the routing table.	0
`user <string>`	Enter the L2TP user name used to connect.	n/a
variables for aggregate and redundant interfaces (models 300A, 310B, 400A, 500A, 620B, and 800 or higher) These variables are available only when `type` **is** `aggregate or redundant`**.**		
`algorithm {L2 | L3 | L4}`	Enter the algorithm used to control how frames are distributed across links in an aggregated interface. The choice of algorithm determines what information is used to determine frame distribution. Enter one of: **L2** — use source and destination MAC addresses. **L3** — use source and destination IP addresses, fall back to L2 algorithm if IP information is not available. **L4** — use TCP, UDP or ESP header information.	`L4`
`lacp-ha-slave {enable | disable}`	This option affects how the aggregate interface participates in Link Aggregation Control Protocol (LACP) negotiation when HA is enabled for the VDOM. It takes effect only if Active-Passive HA is enabled and `lacp-mode` is not `static`. Enter `enable` to participate in LACP negotiation as a `slave` or `disable` to not participate.	`enable`
`lacp-mode {active | passive | static}`	Enter one of active, passive, or static. **`active`** — send LACP PDU packets to negotiate link aggregation connections. This is the default. **`passive`** — respond to LACP PDU packets and negotiate link aggregation connections **`static`** — link aggregation is configured statically	`active`

Variable	Description	Default
`lacp-speed {fast | slow}`	**`slow`** — sends LACP PDU packets every 30 seconds to negotiate link aggregation connections. This is the default. **`fast`** — sends LACP PDU packets every second, as recommended in the IEEE 802.3ad standard. This is available only on FortiGate models 800 and higher when `type` is `aggregate`.	`slow`
`member <if_name1> <if_name2> ...`	Specify a list of physical interfaces that are part of an aggregate or redundant group. To modify a list, enter the complete revised list. If VDOMs are enabled, then `vdom` must be set the same for each interface before you enter the `member` list. An interface is available to be part of an aggregate or redundant group only if • it is a physical interface, not a VLAN interface • it is not already part of an aggregated or redundant interface • it is in the same VDOM as the aggregated interface • it has no defined IP address and is not configured for DHCP or PPPoE • it has no DHCP server or relay configured on it • it does not have any VLAN subinterfaces • it is not referenced in any firewall policy, VIP or multicast policy • it is not an HA heartbeat device or monitored by HA • In a redundant group, failover to the next member interface happens when the active interface fails or is disconnected. The order you specify the interfaces in the `member` list is the order they will become active in the redundant group. For example if you enter `set member port5 port1`, then port5 will be active at the start, and when it fails or is disconnected port1 will become active. This is only available when `type` is `aggregate` or `redundant`.	No default.

Example

This example shows how to set the internal interface IP address and netmask to `192.168.100.159 255.255.255.0`, and the management access to `ping`, `https`, and `ssh`.

```
config system interface
  edit internal
    set allowaccess ping https ssh
    set ip 192.168.110.26 255.255.255.0
  end
```

This example shows how to add a loopback interface with a name of loop1. The IP address is set to 10.0.0.10 255.255.255.0 and bfd is set to global. Any traffic sent to this interface will be dropped, as it is a blackhole route.

```
config system interface
  edit loop1
    set type loopback
    set ip 10.0.0.10 255.255.255.0
    set bfd global
  end
```

This example shows how to configure DHCP on the external interface. The addressing mode is DHCP, the default gateway retrieved from the DHCP server, and the client identifier is changed to “myClientID”. This interface is configured as a DHCP relay agent using non-ipsec with two relay servers configured on this network at 192.168.11.12 and 192.168.11.14.

```
config system interface
  edit external
    set mode dhcp
    set defaultgw enable
    set dhcp-client-identifier myClientID
    set dhcp-relay-service enable
    set dhcp-relay-type regular
    set dhcp-relay-ip 192.168.11.12 192.168.11.14
  end
```

This example shows how to add a secondary IP address and netmask of `192.176.23.180 255.255.255.0` to the internal interface. Also configure `ping` and `https` management access to this secondary IP address. You can not add a secondary IP that is part of the subnet of the original interface IP address.

```
config system interface
  edit internal
    config secondaryip
    edit 1
      set allowaccess ping https
      set ip 192.176.23.180 255.255.255.0
    end
  end
```

History

FortiOS v2.80	Substantially revised. IPv6 added.
FortiOS v2.80 MR2	Added `netbios-forward`, `wins-ip` fields. Removed `zone` field, moved to system zone.
FortiOS v2.80 MR3	Added `defaultgw` field.
FortiOS v2.80 MR6	Added `mtu-override` field.
FortiOS v3.0	Added `ident-accept` field.
FortiOS v3.0 MR1	Added `<pingserver2_ip4>` to `detectserver`, `aggregate` and `redundant` to `type` field, added `pppoe-unnumbered-negotiate` and `priority` fields.
FortiOS v3.0 MR3	DDNS retry interval increased to after 3 failed attempts. Added `wifi-auth, wifi-encrypt,` and `show-backplane-intf` fields. Removed `defaultgw` field.
FortiOS v3.0 MR4	Added `bfd`, `bfd-desired-min-tx`, `bfd-detect-mult`, `bfd-required-min-rx` fields.
FortiOS v3.0 MR5	Added `peer-interface`, `loopback` type, `alias`, `fp-anomaly`, `icmp-redirect`, and `mediatype`. Changes to parameters of `auth-type`.
FortiOS v3.0 MR6	Changed `gateway_address` to `gwaddr`, and `lcp-max-echo-failures` to `lcp-max-echo-fail`. Changed `ipv6-allowaccess` parameters. Added `pptp` variable. Added the `ha-priority` field. Removed all `lt2p-client` commands, and `connection` command.
FortiOS v3.0 MR7	Added `outbandwidth`, IPv6 `autoconf` field, and added `any` option to IPv6 `allowaccess` field. Added `l2tp-client`, and `l2tp-client-settings` subcommands. `dns-server-override` default value is now `enable`.
FortiOS v4.0	Added `nontp-web-proxy`, `ips-sniffer-mode`, and `wccp` fields. Added FortiGate 310B and 610B to models that support aggregate links. Removed `gwaddr`, `mux-type`, `vci`, and `vpi` fields and the `type` field's `adsl` option (no ADSL support).
FortiOS 4.0 MR1	Added the `spillover-threshold`, `dhcp-client-identifier`, `explicit-web-proxy`, and `detectprotocol` fields. Added `hard-switch`, `hdlc`, `vap-switch`, and `vdom-link` types.

ipv6-tunnel

Use this command to tunnel IPv4 traffic over an IPv6 network. The IPv6 interface is configured under `config system interface`. All subnets between the source and destination addresses must support IPv6.

Note: This command is not available in Transparent mode.

Syntax

```
config system ipv6-tunnel
  edit <tunnel_name>
    set destination <remote_IPv6_address>
    set interface <name>
    set source <local_IPv6_address>
  end
```

Variable	Description	Default
`edit <tunnel_name>`	Enter a name for the IPv6 tunnel.	No default.
`destination <remote_IPv6_address>`	The destination IPv6 address for this tunnel.	0.0.0.0
`interface <name>`	The interface used to send and receive traffic for this tunnel.	No default.
`source <local_IPv6_address>`	The source IPv6 address for this tunnel.	0.0.0.0

Example

Use the following commands to set up an IPv6 tunnel.

```
config system ipv6-tunnel
  edit test_tunnel
    set destination 2002:A0A:A01::
    set interface internal
    set source 2002:C0A8:3201::
  end
```

History

FortiOS v2.80 New.

FortiOS v3.0 Changed from ipv6_tunnel to ipv6-tunnel.

FortiOS v3.0 MR1 Removed `vdom` field.

FortiOS v3.0 MR2 Added command syntax for multiple-vdom mode. Removed `ipv6` and `mode` fields.

FortiOS v3.0 MR5 Added `ip6`

FortiOS v3.0 MR6 Removed command.

FortiOS v3.0 MR7 Added command back.

FortiOS v4.0 Removed `ip6` field. Changed `destination` and `source` fields to be IPv6 addresses.

Related topics

- system interface
- system sit-tunnel

mac-address-table

Use this command to create a static MAC table. The table can hold up to 200 entries.

This command is available in Transparent mode only.

Syntax

```
config system mac-address-table
  edit <mac-address_hex>
    set interface <if_name>
  end
```

Variable	Description	Default
`edit <mac-address_hex>`	Enter the MAC address as six pairs of hexadecimal digits separated by colons, e.g.: `11:22:33:00:ff:aa`	No default.
`interface <if_name>`	Enter the name of the interface to which this MAC table entry applies.	No default.

Example

Use the following commands to add a static MAC entry for the internal interface.

```
config system mac-address-table
  edit 11:22:33:00:ff:aa
    set interface internal
  end
```

History

FortiOS v2.80 Renamed and Revised. Formerly `set system brctl`.

modem

Use this command to configure FortiGate models with dedicated modem interfaces or to configure a serial modem interface connected using a serial converter to the USB port.

This command is only available in NAT/Route mode.

You can add the information to connect to up to three dialup accounts. Variables specific to a dialup account end in the number of that dialup account such as `authtype2`, or `passwd3`. A dedicated modem interface can act as a backup interface for one of the FortiGate ethernet interfaces or as a standalone dialup interface.

Modem status is initially set to disabled. Disabled modems will not be displayed in the web-manager interface list. CLI interface lists will always display the modem, no matter what the modem status is. Changing the status to enabled will display the modem in the web-based manager.

Some FortiGate and FortiWifi models have a PCMCIA slot for a 3G wireless modem card. Such a modem can be used as a backup connection in case the land line goes down. The `mode-dev` field allows you to select the 3G modem when its installed, and the `wireless-custom-` fields allow you to configure it.

Syntax

```
config system modem
  set account-relation {equal | fallback}
  set altmode {enable | disable}
  set authtype1 {pap chap mschap mschapv2}
  set authtype2 {pap chap mschap mschapv2}
  set authtype3 {pap chap mschap mschapv2}
  set auto-dial {enable | disable}
  set connect_timeout <seconds>
  set dial-on-demand {enable | disable}
  set distance <distance>
  set extra-init1, extra-init2, extra-init3 <init_str>
  set holddown-timer <seconds>
  set idle-timer <minutes>
  set interface <name>
  set mode {redudant | standalone}
  set modem-dev1, modem-dev2, modem-dev3 {internal | pcmcia-wireless}
  set passwd1, passwd2, passwd3 <password_str>
  set peer_modem1 {actiontec | ascendTNT | generic}
  set peer_modem2 {actiontec | ascendTNT | generic}
  set peer_modem3 {actiontec | ascendTNT | generic}
  set phone1 <phone-number>
  set phone2 <phone-number>
  set phone3 <phone-number>
  set pin-init <init_str>
  set ppp-echo-request1 {disable | enable}
  set ppp-echo-request2 {disable | enable}
  set ppp-echo-request3 {disable | enable}
  set priority <integer> {disable | enable}
  set redial <tries_integer>
  set status {disable | enable}
  set username1 <name_str>
  set username2 <name_str>
  set username3 <name_str>
  set wireless-custom-product-id <pid_hex>
  set wireless-custom-vendor-id <vid_hex>
```

```
    set wireless-port <port_int>
  end
```

Variable	Description	Default
account-relation {equal | fallback}	Set the account relationship as either equal or fallback. **equal** — Accounts are equal and keep using the first successful account. **fallback** — The first account takes priority, fall back to the first account if possible	equal
altmode {enable | disable}	Enable for installations using PPP in China.	enable
authtype1 {pap chap mschap mschapv2} authtype2 {pap chap mschap mschapv2} authtype3 {pap chap mschap mschapv2}	Enter the authentication methods to use for 3G modems as one of: PAP, CHAP, MS-CHAP, or MS-CHAPv2.	pap chap mschap mschapv2
auto-dial {enable | disable}	Enable to dial the modem automatically if the connection is lost or the FortiGate unit is restarted. This is available only when dial-on-demand is set to disabled, and mode is set to standalone.	disable
connect_timeout <seconds>	Set the connection completion timeout (30 - 255 seconds).	90
dial-on-demand {enable | disable}	Enable to dial the modem when packets are routed to the modem interface. The modem disconnects after the idle-timer period. This is available only if auto-dial is set to disabled, and mode is set to standalone.	disable
distance <distance>	Enter the administrative distance (1-255) to use for the default route that is automatically added when the modem connects and obtains an IP address. A lower distance indicates a more preferred route. For more information, see router static "distance <distance>" on page 361. This field is useful for configuring redundant routes in which the modem interface acts as a backup to another interface.	1
extra-init1, extra-init2, extra-init3 <init_str>	Enter up to three extra initialization strings to send to the modem.	null
holddown-timer <seconds>	Used only when the modem is configured as a backup for an interface. Set the time (1-60 seconds) that the FortiGate unit waits before switching from the modem interface to the primary interface, after the primary interface has been restored. This is available only when mode is set to redundant.	60
idle-timer <minutes>	Set the number of minutes the modem connection can be idle before it is disconnected. This is available only if mode is set to standalone.	5
interface <name>	Enter an interface name to associate the modem interface with the ethernet interface that you want to either back up (backup configuration) or replace (standalone configuration).	No default.
mode {redudant | standalone}	Enter the required mode: **redundant** — The modem interface automatically takes over from a selected ethernet interface when that ethernet interface is unavailable. **standalone** — The modem interface is the connection from the FortiGate unit to the Internet.	standalone

Variable	Description	Default
`modem-dev1, modem-dev2, modem-dev3 {internal | pcmcia-wireless}`	modem-dev1/2/3 refers to one of up to 3 configurable modems on your FortiGate unit. Each device can be either `internal` or `pcmcia-wireless` on models that support PCMCIA. The default is `internal`. For 3G PCMCIA modems, select the `pcmcia-wireless` option.	`internal`
`passwd1, passwd2, passwd3 <password_str>`	Enter the password used to access the specified dialup account.	No default.
`peer_modem1 {actiontec | ascendTNT | generic}`	If the modem at `phone1` is Actiontec or AscendTNT, select that type, otherwise leave setting as `generic`. This setting applies to models 50AM, 60M and WiFi-60M only.	`generic`
`peer_modem2 {actiontec | ascendTNT | generic}`	If the modem at `phone2` is Actiontec or AscendTNT, select that type, otherwise leave setting as `generic`. This setting applies to models 50AM, 60M and WiFi-60M only.	`generic`
`peer_modem3 {actiontec | ascendTNT | generic}`	If the modem at `phone3` is Actiontec or AscendTNT, select that type, otherwise leave setting as `generic`. This setting applies to models 50AM, 60M and WiFi-60M only.	`generic`

`phone1 <phone-number>`
`phone2 <phone-number>`
`phone3 <phone-number>`
	Enter the phone number required to connect to the dialup account. Do not add spaces to the phone number. Make sure to include standard special characters for pauses, country codes, and other functions as required by your modem to connect to your dialup account.	No default.

`pin-init <init_str>`	Enter an AT command string to set the PIN. Use this command only after a reboot or major settings change.	`null`
`ppp-echo-request1 {disable | enable}`	Disable `ppp-echo-request1` if the PPP echo request feature is not supported by your wireless ISP. This applies to the 1st modem, if connected. PPP echo request is used to detect low level link down for modems.	`enable`
`ppp-echo-request2 {disable | enable}`	Disable `ppp-echo-request2` if the PPP echo request feature is not supported by your wireless ISP. This applies to a 2nd modem, if connected. PPP echo request is used to detect low level link down for modems.	`enable`
`ppp-echo-request3 {disable | enable}`	Disable `ppp-echo-request3` if the PPP echo request feature is not supported by your wireless ISP. This applies to a 3rd modem, if connected. PPP echo request is used to detect low level link down for modems.	`enable`
`priority <integer> {disable | enable}`	Enter the priority of learned routes on this interface. Valid priorities are from 0 to 4294967295. For more information on route priorities, see “router static” on page 361.	0
`redial <tries_integer>`	Set the maximum number of times (1-10) that the FortiGate unit dials the ISP to restore an active connection on the modem interface. Select `none` to allow the modem to redial without a limit.	No default.
`status {disable | enable}`	Enable or disable modem support. This is equivalent to bringing an interface up or down.	`disable`

`username1 <name_str>`
`username2 <name_str>`
`username3 <name_str>`
	Enter the user name used to access the specified dialup account.	No default.

Variable	Description	Default
`wireless-custom-product-id <pid_hex>`	Configure the product ID of an installed 3G wireless PCMCIA modem. Valid range is 0x0000 - 0xFFFF. This field is available only on models that support PCMCIA cards.	`null`
`wireless-custom-vendor-id <vid_hex>`	Configure the vendor ID of an installed 3G wireless PCMCIA modem. Valid range is 0x0000 - 0xFFFF This field is available only on models that support PCMCIA cards.	`null`
`wireless-port <port_int>`	Enter TTY Port for 3G modems. Enter `0` to use default port.	`0`

Example

This example shows how to enable the modem and configure the modem to act as a backup for the WAN1 interface. Only one dialup account is configured. The FortiGate unit and modem will attempt to dial this account 10 times. The FortiGate unit will wait 5 seconds after the WAN1 interface recovers before switching back to the WAN1 interface.

```
config system modem
  set action dial
  set status enable
  set holddown-timer 5
  set interface wan1
  set passwd1 acct1passwd
  set phone1 1234567891
  set redial 10
  set username1 acct1user
end
```

This example shows how to configure a 3G PCMCIA modem on modem-dev1. There is no authentication used, and this modem device is the Internet connection for the FortiGate unit.

```
config system modem
  set status enable
  set modem-dev1 pcmcia-wireless
  set mode standalone
  set redial 1
  set phone1 " *99***1#"
end
```

History

Related topics

- system interface

npu

Use this command to configure the Network Processing Unit (NPU) for FortiGate units that support FB4. The NPU can take over encryption processing for its interfaces that would normally be performed by the main FortiGate unit CPU.

Note: If you use the traffic-shaping-mode command, the `bidirection` option counts twice as much traffic. You need to allow twice the bandwidth as with unidirection.

Syntax

```
config system npu
    set dec-offload-antireplay {enable | disable}
    set enc-offload-antireplay {enable | disable}
    set offload-ipsec-host {enable | disable}
  next
end
```

Variable	Description	Default
`dec-offload-antireplay {enable | disable}`	Enable this option for the system to offload IPSEC packet encryption to FB4 when the ingress port of the tunnel is on FB4.	`enable`
`enc-offload-antireplay {enable | disable}`	Enable this option for the system to offload IPSEC packet encryption to FB4 when the egress port of the tunnel is on FB4.	`disable`
`offload-ipsec-host {enable | disable}`	Enable this option for the system to offload packet encryption to FB4 when the egress port of this packet is on FB4.	`disable`

History

FortiOS v3.0 MR5 New.

FortiOS v4.0 MR1 Removed `traffic-shaping-mode.`

ntp

Use this command to configure Network Time Protocol (NTP) servers.

Syntax

```
config system ntp
    set ntpsync en/dis
    set syncinterval
    config ntpserver
    edit <serverid>
    set server <IP_address>[/<name_string>]
  next
end
```

Variable	Description	Default
`ntpsync {enable | disable}`	Enable to synchronize FortiGate unit's system time with the ntp server.	`disable`
`syncinterval <interval_int>`	Enter the interval in minutes between contacting NTP server to synchronize time. The range is from 1 to 1440 minutes. Only valid when `ntpsync` is enabled.	`0`
`config ntpserver`	Configure multiple NTP servers	
`edit <serverid_int>`	Enter the number for this NTP server	
`set server <IPv4_addr>[/<hostname_str>`	Enter the IPv4 address and hostname (optional) for this NTP server.	

History

FortiOS v3.0 MR7 New.

password-policy

Use this command to configure higher security requirements for administrator passwords and IPsec VPN pre-shared keys.

Syntax

```
config system password-policy
  set status {enable | disable}
  set apply-to [admin-password ipsec-preshared-key]
  set change-4-characters {enable | disable}
  set expire <days>
  set minimum-length <chars>
  set must-contain [lower-case-letter upper-case-letter non-alphanumeric
     number]
end
```

Variable	Description	Default
`apply-to [admin-password ipsec-preshared-key]`	Select where the policy applies: administrator passwords or IPSec preshared keys.	`admin-password`
`change-4-characters {enable | disable}`	Enable to require the new password to differ from the old password by at least four characters.	`disable`
`expire <days>`	Set time to expiry in days. Enter `0` for no expiry.	`0`
`minimum-length <chars>`	Set the minimum length of password in characters. Range 8 to 32.	`8`
`must-contain [lower-case-letter upper-case-letter non-alphanumeric number]`	Specify character types that must occur at least once in the password.	`Null`
`status {enable | disable}`	Enable password policy.	`disable`

History

FortiOS v4.0 MR1 New.

Related topics

- system admin
- vpn ipsec phase1
- vpn ipsec phase1-interface

proxy-arp

Use this command to add IP addresses to MAC address translation entries to the proxy ARP table.

Syntax

```
config system proxy-arp
  edit <table_entry>
    set interface <port>
    set ip <ipv4_address>
  next
end
```

Variable	Description	Default
`edit <table_entry>`	Enter the unique ID of the table entry to add or modify.	No default.
`interface <port>`	Enter the physical port this IP will be associated with.	No default.
`ip <ipv4_address>`	Enter the IP address to associate with this physical port.	No default.

History

FortiOS v3.0 MR2 New.

Related topics

- system arp-table
- get router info bgp

replacemsg admin

Use this command to change the administration disclaimer page.

If you enter the following CLI command the FortiGate unit displays the Administration Login disclaimer whenever an administrator logs into the FortiGate unit web-based manager or CLI.

```
config system global
  set access-banner enable
end
```

The web-based manager administrator login disclaimer contains the text of the Login Disclaimer replacement message as well as Accept and Decline buttons. The administrator must select accept to login.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg admin admin_disclaimer_text
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
buffer <message>	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
format <format>	Set the format of the message: **html** **text** **none**	No default
header <header_type>	Set the format of the message header: **8bit** **http** **none**	Depends on message type.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message. Generally there is not a large call for these tags in disclaimer pages.

Table 11: Replacement message tags

Tag	Description
%%AUTH_REDIR_URL%%	Link to open a new window. (optional).
%%AUTH_LOGOUT%%	Immediately close the connection policy.
%%KEEPALIVEURL%%	URL the keep alive page connects to that keeps the connection policy alive. Connects every %%TIMEOUT%% seconds.
%%TIMEOUT%%	Configured number of seconds between %%KEEPALIVEURL%% connections.

History

FortiOS v3.0 MR4 New command.

Related Commands

- system global

replacemsg alertmail

The FortiGate unit adds the alert mail replacement messages listed to alert email messages sent to administrators. For more information about alert email, see "system alertemail" on page 392.

Alert mail replacement messages are text messages.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg alertmail alert_msg_type
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
alert_msg_type	FortiGuard replacement alertmail message type. See Table 12.	No default
buffer <message>	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
format <format>	Set the format of the message: **html** **text** **none**	No default
header <header_type>	Set the format of the message header: **8bit** **http** **none**	Depends on message type.

Note: If you enable *Send alert email for logs based on severity* for alert email, whether or not replacement messages are sent by alert email depends on how you set the alert email *Minimum log level*.

Table 12: alertmail message types

Message Type	Description
alertmail-block	*Virus detected* must be enabled for alert email. Antivirus *File Filter* must be enabled in a protection profile, and it must block a file that matches an entry in a selected file filter list.
alertmail-crit-event	Whenever a critical level event log message is generated, this replacement message is sent unless you configure alert email to enable *Send alert email for logs based on severity* and set the *Minimum log level* to *Alert* or *Emergency*.
alertmail-disk-full	*Disk usage* must be enabled, and disk usage reaches the percent full amount configured for alert email. For more information, see "system alertemail" on page 392.
alertmail-nids-event	*Intrusion detected* must be enabled for alert email. When an IPS Sensor or a DoS Sensor detects an attack, this replacement message will be sent.
alertmail-virus	*Virus detected* must be enabled for alert email. Antivirus *Virus Scan* must be enabled in a protection profile and detect a virus.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 13: Replacement message tags

Tag	Description
%%FILE%%	The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages.
%%VIRUS%%	The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages
%%URL%%	The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked.
%%CRITICAL_EVENT%%	Added to alert email critical event email messages. %%CRITICAL_EVENT%% is replaced with the critical event message that triggered the alert email.
%%PROTOCOL%%	The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages.
%%SOURCE_IP%%	IP address of the email server that sent the email containing the virus.
%%DEST_IP%%	IP address of the user's computer that attempted to download the message from which the file was removed.
%%EMAIL_FROM%%	The email address of the sender of the message from which the file was removed.
%%EMAIL_TO%%	The email address of the intended receiver of the message from which the file was removed.
%%NIDS_EVENT%%	The IPS attack message. %%NIDS_EVENT%% is added to alert email intrusion messages.

Example

The default message for a detected virus is:

Virus/Worm detected: %%VIRUS%% Protocol: %%PROTOCOL%% Source IP: %%SOURCE_IP%% Destination IP: %DST_IP%% Email Address From: %%EMAIL_FROM%% Email Address To: %%EMAIL_TO%%

History

FortiOS v2.8 New command.

FortiOS v3.0 MR2 Command removed.

FortiOS v3.0 MR3 Command added. Replacement messages increased in size from 4 096 to 8 192 bytes per message.

Related Commands

- firewall interface-policy
- system alertemail

replacemsg auth

The FortiGate unit uses the text of the authentication replacement messages listed in Table 15 for various user authentication HTML pages that are displayed when a user is required to authenticate because a firewall policy includes at least one identity-based policy that requires firewall users to authenticate. For more information about identity-based policies, see firewall policies in the *FortiOS Administration Guide*.

These pages are used for authentication using HTTP and HTTPS. Authentication replacement messages are HTML messages. You cannot customize the firewall authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

Users see the authentication login page when they use a VPN or a firewall policy that requires authentication. You can customize this page in the same way as you modify other replacement messages,

Administrators see the authentication disclaimer page when logging into the FortiGate web-based manager or CLI. The disclaimer page makes a statement about usage policy to which the user must agree before the FortiGate unit permits access. You should change only the disclaimer text itself, not the HTML form code.

There are some unique requirements for these replacement messages:

- The login page must be an HTML page containing a form with ACTION="/" and METHOD="POST"
- The form must contain the following hidden controls:
  - `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- The form must contain the following visible controls:
  - `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
  - `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg auth auth_msg_type
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
auth_msg_type	FortiGuard replacement message type. See Table 14 on page 481.	No default
buffer <message>	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
format <format>	Set the format of the message: **html** **text** **none**	No default
header <header_type>	Set the format of the message header: **8bit** **http** **none**	Depends on message type.

Table 14: auth message types

Message Type	Description
`auth-challenge-page`	This HTML page is displayed if firewall users are required to answer a question to complete authentication. The page displays the question and includes a field in which to type the answer. This feature is supported by RADIUS and uses the generic RADIUS challenge-access auth response. Usually, challenge-access responses contain a Reply-Message attribute that contains a message for the user (for example, “Please enter new PIN”). This message is displayed on the login challenge page. The user enters a response that is sent back to the RADIUS server to be verified. The Login challenge page is most often used with RSA RADIUS server for RSA SecurID authentication. The login challenge appears when the server needs the user to enter a new PIN. You can customize the replacement message to ask the user for a SecurID PIN. This page uses the %%QUESTION%% tag.
`auth-disclaimer[1|2|3]`	Prompts user to accept the displayed disclaimer when leaving protected network. The web-based manager refers to this as *User Authentication Disclaimer*, and it is enabled with a firewall policy that also includes at least one identity-based policy. When a firewall user attempts to browse a network through the FortiGate unit using HTTP or HTTPS this disclaimer page is displayed. The extra pages seamlessly extend the size of the page from 8 192 characters to 16 384 and 24 576 characters respectively.

`auth-keepalive-page`	The HTML page displayed with firewall authentication keepalive is enabled using the following CLI command:
	`config system global`
	`set auth-keepalive enable`
	`end`
	Authentication keepalive keeps authenticated firewall sessions from ending when the authentication timeout ends. In the web-based manager, go to *User* > *Options* to set the *Authentication Timeout*.
	This page includes %%TIMEOUT%%.

`auth-login-failed-page`	The HTML page displayed if firewall users enter an incorrect user name and password combination. This page includes %%FAILED_MESSAGE%%, %%USERNAMEID%%, and %%PASSWORDID%% tags.
`auth-login-page`	The authentication HTML page displayed when firewall users who are required to authenticate connect through the FortiGate unit using HTTP or HTTPS. Prompts the user for their username and password to login. This page includes %%USERNAMEID%% and %%PASSWORDID%% tags.
`auth-reject-page`	The *Disclaimer page* replacement message does not re-direct the user to a redirect URL or the firewall policy does not include a redirect URL. When a firewall user selects the button on the disclaimer page to decline access through the FortiGate unit, the *Declined disclaimer page* is displayed.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 15: Replacement message tags

Tag	Description
%%AUTH_REDIR_URL%%	Link to open a new window. (optional).
%%AUTH_LOGOUT%%	Immediately close the connection policy.
%%FAILED_MESSAGE%%	Message displayed on failed login page after user login fails.
%%KEEPALIVEURL%%	URL the keep alive page connects to that keeps the connection policy alive. Connects every %%TIMEOUT%% seconds.
%%QUESTION%%	The default login and rejected login pages use this text immediately preceding the username and password fields. The default challenge page uses this as the challenge question. These are treated as two different variables by the server. If you want to use different text, replace %%QUESTION%% with the text that you prefer.
%%TIMEOUT%%	Configured number of seconds between %%KEEPALIVEURL%% connections.
%%USERNAMEID%%	Username of the user logging in. This tag is used on the login and failed login pages.
%%PASSWORDID%%	Password of the user logging in. This tag is used on the challenge, login and failed login pages.

Requirements for login page

The authentication login page is linked to FortiGate functionality and you must construct it according to the following guidelines to ensure that it will work.

- The login page must be an HTML page containing a form with ACTION="/" and METHOD="POST"
- The form must contain the following hidden controls:
- `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
- `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
- `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- The form must contain the following visible controls:
- `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
- `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

Example

This example shows how to change the authentication login page. You enter the web page content as one long quoted string, using the backslash (“\”) character at the end of each line to continue the text on the next line.

```
config system replacemsg auth auth-login-page
  set buffer "<html><head> \
  <title>Firewall Authentication</title> \
  </head> \
  <body><h4>You must authenticate to use this service.</h4> \
  <form action="/" method="post"> \
  <input name="%%MAGICID%%" value="%%MAGICVAL%%" type="hidden"> \
  <table align="center" bgcolor="#00cccc" border="0" \
  cellpadding="15" cellspacing="0" width="320"><tbody> \
  <tr><th>Username:</th> \
  <td><input name="%%USERNAMEID%%" size="25" type="text"></td></tr> \
  <tr><th>Password:</th> \
  <td><input name="%%PASSWORDID%%" size="25" type="password"></td> \
  </tr><tr><td colspan="2" align="center" bgcolor="#00cccc"> \
```

```
    <input name="%%STATEID%%" value="%%STATEVAL%%" type="hidden"> \
    <input name="%%REDIRID%%" value="%%PROTURI%%" type="hidden"> \
    <input value="Continue" type="submit"></td></tr></tbody></table> \
    </font></form></body></html>"
    set format html
    set header http
  end
```

History

FortiOS v3.0	`auth` category added.
FortiOS v3.0 MR2	Added `auth-challenge-page`, `auth-disclaimer[1|2|3]-page`, `auth-keepalive-page`, `auth-loginfailed-page` and `auth-reject-page fields`.
FortiOS v3.0 MR3	Replacement messages increased in size from 4 096 to 8 192 bytes per message.

Related Commands

- system global

replacemsg ec

The endpoint control (ec) replacement messages format the portal pages that the FortiGate unit sends to non-compliant users who attempt to use a firewall policy in which Endpoint NAC (`endpoint-check`) is enabled.

There are two Endpoint NAC portals:

- *Endpoint NAC Download Portal* — The FortiGate unit sends this page if the Endpoint NAC profile has `recommendation-disclaimer` disabled. In the web-based manager, this is the *Quarantine Hosts to User Portal (Enforce compliance)* option. The user can download the FortiClient Endpoint Security application installer. If you modify this replacement message, be sure to retain the `%%LINK%%` tag which provides the download URL for the FortiClient installer.
- *Endpoint NAC Recommendation Portal* — The FortiGate unit sends this page if the Endpoint NAC profile has `recommendation-disclaimer` enabled. In the web-based manager, this is the *Notify Hosts to Install FortiClient (Warn only)* option. The user can either download the FortiClient Endpoint Security application installer or select the *Continue to* link to access their desired destination. If you modify this replacement message, be sure to retain both the `%%LINK%%` tag which provides the download URL for the FortiClient installer and the `%%DST_ADDR%%` link that contains the URL that the user requested.

Message format is HTML by default.

Syntax

```
config system replacemsg ec endpt-download-portal
  set buffer <message>
  set format <format>
  set header <header_type>
end
config system replacemsg ec endpt-recommendation-portal
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
`endpt-download-portal`	The Endpoint NAC Download Portal. The FortiGate unit sends this message to non-compliant users if `recommendation-disclaimer` is disabled in the Endpoint Control profile. The user can download the FortiClient Endpoint Security application installer.	No default
`endpt-recommendation-portal`	The Endpoint NAC Recommendation Portal. The FortiGate unit sends this message to non-compliant users if `recommendation-disclaimer` is enabled in the Endpoint Control profile. The user can either download the FortiClient Endpoint Security application installer or select the *Continue to* link to access their desired destination.	No default
`buffer <message>`	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.

Variable	Description	Default
`format <format>`	Set the format of the message: **`html`** **`text`** **`none`**	
`header <header_type>`	Set the format of the message header: **`8bit`** **`http`** **`none`**	

The endpoint control replacement messages include the following replacement message tags. When users receive the replacement message, the replacement message tag is replaced with the appropriate content.

Table 16: Replacement message tags

Tag	Description
`%%LINK%%`	The download URL for the FortiClient installer.
`%%DST_ADDR%%`	The destination URL that the user entered. This is used in the `endpt-recommendation-portal` message only.

History

FortiOS v4.0 New

FortiOS v4.0 MR1 `endpt-recommendation-portal` message and `%%DST_ADDR%%` message tag added.

Related topics

- endpoint-control profile
- firewall policy, policy6

replacemsg fortiguard-wf

Use this command to change the default messages that replace a web pages that FortiGuard web filtering has blocked.

The FortiGate unit sends the FortiGuard Web Filtering replacement messages listed in Table 17 to web browsers using the HTTP protocol when FortiGuard web filtering blocks a URL, provides details about blocked HTTP 4xx and 5xx errors, and for FortiGuard overrides. FortiGuard Web Filtering replacement messages are HTTP pages.

If the FortiGate unit supports SSL content scanning and inspection and if *Protocol Recognition* > *HTTPS Content Filtering Mode* is set to Deep Scan in the protection profile, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

By default, these are HTML messages.

Syntax

```
config system replacemsg fortiguard-wf <fortiguard_msg_type>
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
`<fortiguard_msg_type>`	FortiGuard replacement message type. See Table 17.	No default.
`buffer <message>`	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
`format <format>`	Set the format of the message: **`html`** **`text`** **`none`**	No default
`header <header_type>`	Set the format of the message header: **`8bit`** **`http`** **`none`**	Depends on message type.

Table 17: FortiGuard Web Filtering replacement messages

Message name	Description
`ftgd-block`	*Enable FortiGuard Web Filtering* is enabled in a protection profile for HTTP or HTTPS, and blocks a web page. The blocked page is replaced with the `ftgd-block` web page.
`ftgd-ovrd`	Override selected filtering for a FortiGuard Web Filtering category and FortiGuard Web Filtering blocks a web page in this category. displays this web page. Using this web page users can authenticate to get access to the page. Go to *UTM* > *Web Filter* > *Override* to add override rules. For more information, see "webfilter ftgd-ovrd" on page 668. The `%%OVRD_FORM%%` tag provides the form used to initiate an override if FortiGuard Web Filtering blocks access to a web page. Do not remove this tag from the replacement message.
`http-err`	*Provide details for blocked HTTP 4xx and 5xx errors* is enabled in a protection profile for HTTP or HTTPS, and blocks a web page. The blocked page is replaced with the `http-err` web page.

History

FortiOS v2.80	New
FortiOS v2.80 MR2	Changed `cerb` field to `catblock`.

FortiOS v3.0	IM category added.
	Changed:
	`fortiguard_wf` to `fortiguard-wf`
	`ftgd_block` to `ftgd-block`
	`ftgd_ovrd` to `ftgd-ovrd`
	`http_err` to `http-err`

FortiOS v3.0 MR3	Replacement messages increased in size from 4 096 to 8 192 bytes per message.

Related Commands

- webfilter

replacemsg ftp

The FortiGate unit sends the FTP replacement messages to FTP clients when an event occurs such as antivirus blocking a file that contains a virus in an FTP session.

By default, these are text-format messages with no header.

Syntax

```
config system replacemsg ftp <message-type>
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
`<message-type>`	FTP replacement message type. See Table 18.	No default.
`buffer <message>`	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
`format <format>`	Set the format of the message: **`html`** **`text`** **`none`**	No default
`header <header_type>`	Set the format of the message header: **`8bit`** **`http`** **`none`**	Depends on message type.

Table 18: FTP replacement messages

Message name	Description
`ftp-dl-blocked`	Antivirus *File Filter* enabled for FTP in a protection profile blocks a file being downloaded using FTP that matches an entry in the selected file filter list and sends this message to the FTP client.
`ftp-dl-dlp`	In a DLP sensor, a rule with action set to *Block* replaces a blocked FTP download with this message.
`ftp-dl-dlp-ban`	In a DLP sensor, a rule with action set to *Ban* blocks an FTP session and displays this message. This message is displayed whenever the banned user attempts to access until the user is removed from the banned user list.
`ftp-dl-filesize`	Antivirus *Oversized File/Email* set to *Block* for FTP in a protection profile blocks an oversize file from being downloaded using FTP and sends this message to the FTP client.
`ftp-dl-infected`	Antivirus *Virus Scan* is enabled for FTP in a protection profile, and it deletes an infected file being downloaded using FTP. The `ftp-dl-infected` message is sent to the FTP client.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 19: Replacement message tags

Tag	Description
%%FILE%%	The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages.
%%VIRUS%%	The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages
%%QUARFILENAME%%	The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.
%%URL%%	The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked.
%%PROTOCOL%%	The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages.
%%SOURCE_IP%%	The IP address from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of the web page that sent the virus.
%%DEST_IP%%	The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed.

Example

This example shows how to change the message sent when an FTP download is oversize.

```
config system replacemsg ftp ftp-dl-filesize
  set buffer "The downloaded file was blocked because it is > 10MB."
end
```

History

FortiOS v2.80 New

FortiOS v3.0 MR3 Replacement messages increased in size from 4 096 to 8 192 bytes per message.

replacemsg http

Use this command to change default replacement messages added to web pages when the antivirus engine blocks a file in an HTTP session because of a matching file pattern or because a virus is detected; or when web filter blocks a web page.

The FortiGate unit sends the HTTP replacement messages listed to web browsers using the HTTP protocol when an event occurs such as antivirus blocking a file that contains a virus in an HTTP session. HTTP replacement messages are HTML pages.

If the FortiGate unit supports SSL content scanning and inspection and if *Protocol Recognition* > *HTTPS Content Filtering Mode* in the web-manager is set to Deep Scan in the protection profile, these replacement messages can also replace web pages downloaded using the HTTPS protocol.

Syntax

```
config system replacemsg http <message-type>
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
`<message-type>`	HTTP replacement message type. See Table 20.	No default.
`buffer <message>`	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
`format <format>`	Set the format of the message: **`html`** **`text`** **`none`**	No default
`header <header_type>`	Set the format of the message header: **`8bit`** **`http`** **`none`**	Depends on message type.

Table 20: HTTP replacement messages

Message name	Description
`bannedword`	Web content blocking is enabled in a protection profile, and blocks a web page being downloaded with an HTTP GET that contains content matching an entry in the selected Web Content Block list. The blocked page is replaced with the `bannedword` web page.
`http-block`	Antivirus *File Filter* is enabled for HTTP or HTTPS in a protection profile, and blocks a file being downloaded using an HTTP GET that matches an entry in the selected file filter list. The file is replaced with the `http-block` web page that is displayed by the client browser.
`http-client-bannedword`	Web content blocking enabled in a protection profile blocks a web page being uploaded with an HTTP PUT that contains content that matches an entry in the selected Web Content Block list. The client browser displays the `http-client-bannedword` web page.
`http-client-block`	Antivirus *File Filter* is enabled for HTTP or HTTPS in a protection profile blocks a file being uploaded by an HTTP POST that matches an entry in the selected file filter list and replaces it with the `http-client-block` web page that is displayed by the client browser.
`http-client-virus`	Antivirus *Virus Scan* is enabled for HTTP or HTTPS in a protection profile deletes an infected file being uploaded using an HTTP PUT and replaces the file with this a web page that is displayed by the client browser.

Table 20: HTTP replacement messages

Message name	Description
http-client-filesize	In a protection profile, antivirus *Oversized File/Email* is set to *Block* for HTTP or HTTPS and an oversized file that is being uploaded with an HTTP PUT is blocked and replaced with the `http-client-filesize` web page.
http-contenttype-block	In a protection profile, when a specific type of content is not allowed, it is replaced with the `http-contenttype-block` web page.
http-dlp	In a DLP sensor, a rule with action set to *Block* replaces a blocked web page or file with the `http-dlp` web page.
http-dlp-ban	In a DLP sensor, a rule with action set to *Ban* replaces a blocked web page or file with the `http-dlp-ban` web page. This web page also replaces any additional web pages or files that the banned user attempts to access until the user is removed from the banned user list.
http-filesize	Antivirus *Oversized File/Email* is set to *Block* for HTTP or HTTPS in a protection profile, and blocks an oversized file being downloaded using an HTTP GET. The file is replaced with the `http-filesize` web page that is displayed by the client browser.
http-post-block	*HTTP POST Action* is set to *Block* in a protection profile and the FortiGate unit blocks an HTTP POST and displays the `http-post-block` web page.
http-virus	Antivirus *Virus Scan* is enabled for HTTP or HTTPS in a protection profile. It deletes an infected file that is being downloaded using an HTTP GET and replaces the file with the `http-virus` web page that is displayed by the client browser.
infcache-block	Client comforting is enabled in a protection profile and the FortiGate unit blocks a URL added to the client comforting URL cache. It replaces the blocked URL with the `infcache-block` web page. For more information about the client comforting URL cache, see"firewall policy, policy6" on page 129.
url-block	Web URL filtering is enabled in a protection profile, and blocks a web page with a URL that matches an entry in the selected URL Filter list. The blocked page is replaced with the `url-block` web page.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 21: Replacement message tags

Tag	Description
%%FILE%%	The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages.
%%VIRUS%%	The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages
%%QUARFILENAME%%	The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.
%%URL%%	The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked.
%%PROTOCOL%%	The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages.
%%SOURCE_IP%%	The IP address of the web page from which a virus was received.
%%DEST_IP%%	The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed.

Example

This example shows how to change the message that replaces a web page blocked for banned words.

```
config system replacemsg http http-client-bannedword
  set buffer "This web page was blocked. It contains banned words."
end
```

History

FortiOS v2.80	New
FortiOS v3.0 MR2	Added infcache-block replacemsg.
FortiOS v3.0 MR3	Replacement messages increased in size from 4 096 to 8 192 bytes per message.
FortiOS v4.0 MR1	Added `http-contenttypeblock` message type.

replacemsg im

Use this command to change default replacement messages added to instant messaging and peer-to-peer sessions when either file-transfer or voice-chat is blocked.

By default, these are text messages with an 8-bit header.

Syntax

```
config system replacemsg im <message-type>
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
<message-type>	im replacement message type. See Table 22.	No default.
buffer <message>	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
format <format>	Set the format of the message: **html** **text** **none**	No default
header <header_type>	Set the format of the message header: **8bit** **http** **none**	Depends on message type.

Table 22: Instant messaging (IM) and peer to peer (P2P) message types

Message name	Description
im-dlp	In a DLP sensor, a rule with action set to *Block* replaces a blocked IM or P2P message with this message.
im-dlp-ban	In a DLP sensor, a rule with action set to *Ban* replaces a blocked IM or P2P message with this message. This message also replaces any additional messages that the banned user sends until they are removed from the banned user list.
im-file-xfer-block	Antivirus *File Filter* enabled for IM in a protection profile deletes a file that matches an entry in the selected file filter list and replaces it with this message.
im-file-xfer-infected	Antivirus *Virus Scan* enabled for IM in a protection profile deletes a infected file from and replaces the file with this message.
im-file-xfer-name	Antivirus *File Filter* enabled for IM in a protection profile deletes a file with a name that matches an entry in the selected file filter list and replaces it with this message.
im-file-xfer-size	Antivirus *Oversized File/Email* set to *Block* for IM in a protection profile removes an oversized file and replaces the file with this message.
im-long-chat-block	In an Application Control list, the block-long-chat CLI field is enabled for AIM, ICQ, MSN, or Yahoo and the application control list is added to a protection profile. You enable blocking oversized chat messages from the CLI.
im-photo-share-block	In an Application Control list, the block-photo CLI field is enabled for MSN, or Yahoo and the application control list is added to a protection profile. You enable photo blocking from the CLI.
im-voice-chat-block	In an Application Control list, the *Block Audio* option is selected for AIM, ICQ, MSN, or Yahoo! and the application control list is added to a protection profile.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 23: Replacement message tags

Tag	Description
%%FILE%%	The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages.
%%VIRUS%%	The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages
%%QUARFILENAME%%	The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.
%%PROTOCOL%%	The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages.
%%SOURCE_IP%%	The IP address from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of the web page that sent the virus.
%%DEST_IP%%	The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed.

Example

This example shows how to change the message added to instant messaging sessions when voice chat is blocked.

```
config system replacemsg im im-voice-chat-block
  set buffer "Use of chat applications is not permitted."
end
```

History

FortiOS v2.80	New
FortiOS v3.0	IM category added.
FortiOS v3.0 MR3	Replacement messages increased in size from 4 096 to 8 192 bytes per message.
FortiOS v4.0 MR1	Added `im-long-chat-block` message type.

replacemsg mail

Use this command to change default replacement messages added to email messages when the antivirus engine blocks a file either because of a matching file pattern or because a virus is detected; or when spam filter blocks an email.

By default, these are text messages with an 8-bit header.

Syntax

```
config system replacemsg mail <message-type>
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
<message-type>	mail replacement message type. See Table 24.	No default.
buffer <message>	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
format <format>	Set the format of the message: **html** **text** **none**	No default
header <header_type>	Set the format of the message header: **8bit** **http** **none**	Depends on message type.

Table 24: mail message types

Message name	Description
email-block	The antivirus *File Filter* is enabled for an email protocol in a protection profile, and deletes a file that matches an entry in the selected file filter list. The file is blocked and the email is replaced with the email-block message.
email-dlp	In a DLP sensor, a rule with action set to *Block* replaces a blocked email message with the email-dlp message.
email-dlp-ban	In a DLP sensor, a rule with action set to *Ban* replaces a blocked email message with this message. This message also replaces any additional email messages that the banned user sends until they are removed from the banned user list.
email-dl-ban-sender	In a DLP sensor, a rule with action set to *Ban Sender* replaces a blocked email message with this message. The email-dlp-ban message also replaces any additional email messages that the banned user sends until the user is removed from the banned user list.
email-dlp-subject	The email-dlp-subject message is added to the subject field of all email messages replaced by the DLP sensor *Block*, *Ban*, *Ban Sender*, *Quarantine IP address*, and *Quarantine interface* actions.
email-filesize	When the antivirus *Oversized File/Email* is set to *Block* for an email protocol in a protection profile and removes an oversized file from an email message, the file is replaced with the email-filesize message.
email-virus	Antivirus *Virus Scan* is enabled for an email protocol in a protection profile, it deletes an infected file from an email message and replaces the file with the email-virus message.

Table 24: mail message types

Message name	Description
partial	In a protection profile, antivirus *Pass Fragmented Emails* is not enabled so a fragmented email is blocked. The partial message replaces the first fragment of the fragmented email.
smtp-block	Splice mode is enabled and the antivirus file filter deleted a file from an SMTP email message. The FortiGate unit aborts the SMTP session and returns a 554 SMTP error message to the sender that includes the smtp-block replacement message.
smtp-filesize	Splice mode is enabled and antivirus *Oversized File/Email* is set to *Block*. When the FortiGate unit blocks an oversize SMTP email message, the FortiGate unit aborts the SMTP session and returns a 554 SMTP error message to the sender that includes the smtp-filesize replacement message.
smtp-virus	Splice mode is enabled and the antivirus system detects a virus in an SMTP email message. The FortiGate unit aborts the SMTP session and returns a 554 SMTP error message to the sender that includes the smtp-virus replacement message.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 25: Replacement message tags

Tag	Description
%%FILE%%	The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages.
%%VIRUS%%	The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages
%%QUARFILENAME%%	The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.
%%PROTOCOL%%	The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages.
%%SOURCE_IP%%	IP address of the email server that sent the email containing the virus.
%%DEST_IP%%	IP address of the user's computer that attempted to download the message from which the file was removed.
%%EMAIL_FROM%%	The email address of the sender of the message from which the file was removed.
%%EMAIL_TO%%	The email address of the intended receiver of the message from which the file was removed.

Example

This example shows how to change the email message that is sent to test the alert email system.

```
config system replacemsg mail email-virus
  set buffer "The attachment was blocked because it contains a virus."
end
```

History

FortiOS v2.80	New
FortiOS v3.0 MR3	Replacement messages increased in size from 4 096 to 8 192 bytes per message.
FortiOS v4.0	Added email-dlp, email-dlp-ban, email-dlp-ban-sender, and email-dlp-subject message types.

replacemsg-group

Use this command to define replacement messages for your VDOM, overriding the corresponding global replacement messages.

Syntax

To create a VDOM-specific replacement message:

```
config system replacemsg-group
  edit default
    config <msg_category>
      edit <msg_type>
        set buffer <message>
        set format <format>
        set header <header_type>
      end
    end
```

To remove a VDOM-specific replacement message, restoring the global replacement message:

```
config system replacemsg-group
  edit default
    config <msg_category>
      delete <msg_type>
    end
```

Variable	Description	Default
`buffer <message>`	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.

`format <format>`	Set the format of the message:
	`html`
	`text`
	`none`
		No default

`header <header_type>`	Set the format of the message header:
	`8bit`
	`http`
	`none`
		Depends on message type.

`<msg_category>`	The category of replacement message. This corresponds to the field following `replacemsg` in the global `system replacemsg` command. For example, the `http` category includes the messages defined globally in the `system replacemsg http` command.	No default
`<msg_type>`	The message type. This corresponds to the final field in the global `system replacemsg` command. For example, to create a new login message for your SSL VPN, you would set `<msg_category>` to `sslvpn` and `<msg_type>` to `sslvpn-login`.	No default

History

FortiOS v4.0 MR1 New.

replacemsg nac-quar

Use this command to change the NAC quarantine pages for data leak (DLP), denial of service (DoS), IPS, and virus detected.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg auth auth_msg_type
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
nac-quar_msg_type	Replacement message type. See Table 26.	No default
buffer <message>	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
format <format>	Set the format of the message: html text none	No default
header <header_type>	Set the format of the message header: 8bit http none	Depends on message type.

Table 26: nac-quar message types

Message name	Description
nac-quar-dlp	*Action* set to *Quarantine IP address* or *Quarantine Interface* in a DLP sensor and the DLP sensor added to a protection profile adds a source IP address or a FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80.
nac-quar-dos	For a DoS Sensor the CLI quarantine option set to attacker or interface and the DoS Sensor added to a DoS firewall policy adds a source IP, a destination IP, or FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80. This replacement message is not displayed if quarantine is set to both.
nac-quar-ips	*Quarantine Attackers* enabled in an IPS sensor filter or override and the IPS sensor added to a protection profile adds a source IP address, a destination IP address, or a FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80. This replacement message is not displayed if *method* is set to *Attacker and Victim IP Address*.
nac-quar-virus	Antivirus *Quarantine Virus Sender* enabled in a protection profile adds a source IP address or FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80.

History

FortiOS v4.0 `nac-quar` category added.

replacemsg nntp

Use this command to change the net news transfer protocol (NNTP) download pages.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg nntp auth_msg_type
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
auth_msg_type	FortiGuard replacement alertmail message type. See Table 27.	No default
buffer <message>	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
format <format>	Set the format of the message: html text none	No default
header <header_type>	Set the format of the message header: 8bit http none	Depends on message type.

Table 27: net news transfer protocol (NNTP) message types

Message name	Description
nntp-dl-blocked	Antivirus *File Filter* is enabled for NNTP in a protection profile, and blocks a file attached to an NNTP message that matches an entry in the selected file filter list. The FortiGate unit sends the nntp-dl-blocked message to the FTP client.
nntp-dl-filesize	Antivirus *Oversized File/Email* is set to *Block* for NNTP in a protection profile. The FortiGate unit removes an oversized file from an NNTP message and replaces the file with the nntp-dl-filesize message.
nntp-dl-infected	Antivirus *Virus Scan* is enabled for NTTP in a protection profile that deletes an infected file attached to an NNTP message and sends the nntp-dl-infected message to the FTP client.
nntp-dlp	In a DLP sensor, a rule with action set to *Block* replaces a blocked NNTP message with the nntp-dlp message.
nntp-dlp-ban	In a DLP sensor, a rule with action set to *Ban* replaces a blocked NNTP message with this message. The nntp-dlp-ban message also replaces any additional NNTP messages that the banned user sends until they are removed from the banned user list.
nntp-dlp-subject	The nntp-dlp-subject message is added to the subject field of all NNTP messages replaced by the DLP sensor *Block*, *Ban*, *Quarantine IP address*, and *Quarantine interface* actions.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 28: Replacement message tags

Tag	Description
%%FILE%%	The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. The file may have been quarantined if a virus was detected. %%FILE%% can be used in virus and file block messages.
%%QUARFILENAME%%	The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.
%%VIRUS%%	The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages

Example

The default message for a detected virus is:

Virus/Worm detected: %%VIRUS%% Protocol: %%PROTOCOL%% Source IP: %%SOURCE_IP%% Destination IP: %DST_IP%% Email Address From: %%EMAIL_FROM%% Email Address To: %%EMAIL_TO%%

History

FortiOS v3.0 MR4 New command.

replacemsg spam

The FortiGate unit adds the Spam replacement messages listed in Table 29 to SMTP server responses if the email message is identified as spam and the spam action is discard. If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also be added to SMTPS server responses.

By default, these are text messages with an 8-bit header.

Syntax

```
config system replacemsg spam <message-type>
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
<message-type>	Spam replacement message type. See Table 29.	No default.
buffer <message>	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.
format <format>	Set the format of the message, one of: html text none	text
header <header_type>	Set the format of the message header, one of: 8bit http none	8bit

Table 29: spam message types

Message name	Description
ipblocklist	Spam Filtering *IP address BWL check* enabled for an email protocol in a protection profile identifies an email message as spam and adds this replacement message.
reversedns	Spam Filtering *Return e-mail DNS check* enabled for an email protocol in a protection profile identifies an email message as spam and adds this replacement message.
smtp-spam-ase	The FortiGuard Antispam Engine (ASE) reports this message as spam.
smtp-spam-bannedword	Spam Filtering *Banned word check* enabled for an email protocol in a protection profile identifies an email message as spam and adds this replacement message.
smtp-spam-dnsbl	From the CLI, spamrbl enabled for an email protocol in a protection profile identifies an email message as spam and adds this replacement message.
smtp-spam-emailblack	The spam filter email address blacklist marked an email as spam. The smtp-spam-emailblack replaces the email.
smtp-spam-feip	FortiGuard Antispam IP address checking identifies an email message as spam and adds this replacement message to the server response.
smtp-spam-helo	Spam Filtering *HELO DNS lookup* enabled for SMTP in a protection profile identifies an email message as spam and adds this replacement message. *HELO DNS lookup* is not available for SMTPS.
smtp-spam-mimeheader	From the CLI, spamhdrcheck enabled for an email protocol in a protection profile identifies an email message as spam and adds this replacement message.

Table 29: spam message types

Message name	Description
submit	Any Spam Filtering option enabled for an email protocol in a protection profile identifies an email message as spam and adds this replacement message. Spam Filtering adds this message to all email tagged as spam. The message describes a button that the recipient of the message can select to submit the email signatures to the FortiGuard Antispam service if the email was incorrectly tagged as spam (a false positive).

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 30: Replacement message tags

Tag	Description
%%QUARFILENAME%%	The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.
%%SOURCE_IP%%	The IP address from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of the web page that sent the virus.
%%DEST_IP%%	The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed.
%%EMAIL_FROM%%	The email address of the sender of the message from which the file was removed.
%%EMAIL_TO%%	The email address of the intended receiver of the message from which the file was removed.

Example

This example shows how to change the message added to SMTP mail that the spam filter has blocked.

```
config system replacemsg spam ipblocklist
  set buffer "This email was blocked as spam."
end
```

History

FortiOS v2.80 New

FortiOS v3.0 MR2 Added `smtp-spam-fschksum` replacement message.

FortiOS v3.0 MR3 Replacement messages increased in size from 4 096 to 8 192 bytes per message.

FortiOS v4.0 Added `smtp-spam-ase` and `smtp-spam-dnsbl` replacement messages.

replacemsg sslvpn

The SSL VPN login replacement messages are HTML replacement messages.

The `sslvpn-logon` message formats the FortiGate SSL VPN portal login page.

The `sslvpn-limit` message formats the web page that appears if a user attempts to log into SSL VPN more than once.

You can customize these replacement messages according to your organization's needs. The pages are linked to FortiGate functionality and you must construct them according to the following guidelines to ensure that it will work.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg sslvpn {sslvpn-limit | sslvpn-logon}
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
`buffer <message>`	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.

`format <format>`	Set the format of the message:
	`html`
	`text`
	`none`
		No default

`header <header_type>`	Set the format of the message header:
	`8bit`
	`http`
	`none`
		Depends on message type.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Requirements for SSL VPN HTML pages

The SSL pages are linked to FortiGate functionality and you must construct them according to the following guidelines to ensure that it will work.

- The pages must be HTML pages containing a form with ACTION="%%SSL_ACT%%" and METHOD="%%SSL_METHOD%%"
- The form must contain the %%SSL_LOGIN%% tag to provide the logon form.
- The form must contain the %%SSL_HIDDEN%% tag.

History

FortiOS v3.0 sslvpn replacemsg category added.

FortiOS v3.0 MR3 Replacement messages increased in size from 4 096 to 8 192 bytes per message.

replacemsg traffic-quota

When user traffic through the FortiGate unit is blocked by traffic shaper quota controls, users see the *Traffic shaper block message* or the P*er IP traffic shaper block message* when they attempt to connect through the FortiGate unit using HTTP.

This is an HTML message with an HTTP header.

Syntax

```
config system replacemsg traffic-quota {per-ip-shaper-block | traffic-
   shaper-block}
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

Variable	Description	Default
`buffer <message>`	Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters.	Depends on message type.

`format <format>`	Set the format of the message:
	`html`
	`text`
	`none`
		No default

`header <header_type>`	Set the format of the message header:
	`8bit`
	`http`
	`none`
		Depends on message type.

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Requirements for traffic quota pages

The traffic quota HTTP pages should contain the %%QUOTA_INFO%% tag to display information about the traffic shaping quota setting that is blocking the user.

History

FortiOS v4.0 MR1 New

resource-limits

Use this command to configure resource limits that will apply to all VDOMs. When you set a global resource limit, you cannot exceed that resource limit in any VDOM. For example, enter the following command to limit all VDOMS to 100 VPN IPSec Phase 1 Tunnels:

```
config global
  config system resource-limits
    set ipsec-phase1 100
  end
end
```

With this global limit set you can only add a maximum of 100 VPN IPSec Phase 1 Tunnels to any VDOM.

You can also edit the resource limits for individual VDOMs to further limit the number of resources that you can add to individual VDOMs. See "system vdom-property" on page 535.

A resource limit of 0 means no limit. No limit means the resource is not being limited by the resource limit configuration. Instead the resource is being limited by other factors. The FortiGate unit limits dynamic resources by the capacity of the FortiGate unit and can vary depending on how busy the system is. Limits for static resources are set by limitations in the FortiGate configuration as documented in the *FortiGate Maximum Values Matrix* document.

The default maximum value for each resource depends on the FortiGate model. Dynamic resources (Sessions, Dial-up Tunnels, and SSL VPN) do not have default maximums so the default maximum for dynamic resources is always 0 (meaning unlimited). Static resources may have a limit set or many be set to 0 meaning they are limited by the resource limit configuration.

Note: If you set the maximum resource usage for a VDOM you cannot reduce the default maximum global limit for all VDOMs below this maximum.

This command is available only when VDOMs are enabled.

Syntax

```
config global
  config system resource-limits
    set custom-service <max_int>
    set dialup-tunnel <max_int>
    set firewall-address <max_int>
    set firewall-addrgrp <max_int>
    set firewall-policy <max_int>
    set firewall-profile <max_int>
    set ipsec-phase1 <max_int>
    set ipsec-phase2 <max_int>
    set onetime-schedule <max_int>
    set recurring-schedule <max_int>
    set service-group <max_int>
    set session <max_int>
    set sslvpn <max_int>
    set user <max_int>
    set user-group <max_int>
  end
end
```

Variable	Description	Default
`custom-service <max_int>`	Enter the maximum number of firewall custom services.	
`dialup-tunnel <max_int>`	Enter the maximum number of dialup-tunnels.	
`firewall-address <max_int>`	Enter the maximum number of firewall addresses.	
`firewall-addrgrp <max_int>`	Enter the maximum number of firewall address groups.	
`firewall-policy <max_int>`	Enter the maximum number of firewall policies.	
`firewall-profile <max_int>`	Enter the maximum number of firewall profiles.	
`ipsec-phase1 <max_int>`	Enter the maximum number of IPSec phase1 tunnels.	
`ipsec-phase2 <max_int>`	Enter the maximum number of IPSec phase2 tunnels.	
`onetime-schedule <max_int>`	Enter the maximum number of onetime schedules.	
`recurring-schedule <max_int>`	Enter the maximum number of recurring schedules.	
`service-group <max_int>`	Enter the maximum number of firewall service groups.	
`session <max_int>`	Enter the maximum number of sessions.	
`sslvpn <max_int>`	Enter the maximum number of sessions.	
`user <max_int>`	Enter the maximum number of users.	
`user-group <max_int>`	Enter the maximum number of user groups.	

History

FortiOS v4.0 New.

Related Commands

- system vdom-property

session-helper

A session helper binds a service to a TCP or UDP port. By default, there are session helpers that bind services to standard ports. Use this command to configure a new session helper or to edit an existing one.

Syntax

```
config system session-helper
  edit <helper-number>
    set name <helper-name>
    set port <port_number>
    set protocol <protocol_number>
  end
```

Table 31: Services, ports, and protocols

1	pptp	port 1723	protocol 6
2	h323	port 1720	protocol 6
3	ras	port 1719	protocol 17
4	tns	port 1521	protocol 6
5	tftp	port 69	protocol 17
6	rtsp	port 23	protocol 6
7	rtsp	port 25	protocol 6
8	ftp	port 21	protocol 6
9	rtsp	port 554	protocol 6
10	rtsp	port 7070	protocol 6

11	pmap	port 111	protocol 17
12	sip	5060	protocol 17
13	dns-udp	53	protocol 17
14	rsh	514	protocol 6
15	rsh	512	protocol 6
16	dcerpc	135	protocol 6
17	dcerpc	135	protocol 17
18	mgcp	2427	protocol 17
19	mgcp	2727	protocol 17

Variable	Description	Default
`<helper-number>`	Enter the number of the session-helper that you want to edit, or enter an unused number to create a new session-helper.	No default.
`name <helper-name>`	The name of the session helper. One of: dcerpc, dns-tcp, dns-udp, ftp, h245I, h245O, h323, ident, mms, pmap, pptp, ras, rsh, rtsp, sip, tftp, tns.	No default.
`port <port_number>`	Enter the port number to use for this protocol.	No default.
`protocol <protocol_number>`	The protocol number for this service, as defined in RFC 1700.	No default.

Example

Use the following commands to edit the file transfer protocol (FTP) and change it to port 111, but remain as protocol 6:

```
config system session-helper
  edit 8
    set name ftp
    set port 111
    set protocol 6
  end
```

History

FortiOS v2.80 New

FortiOS v3.0 Changed `dns_tcp` to `dns-tcp` and `dns_udp` to `dns-udp`.

session-sync

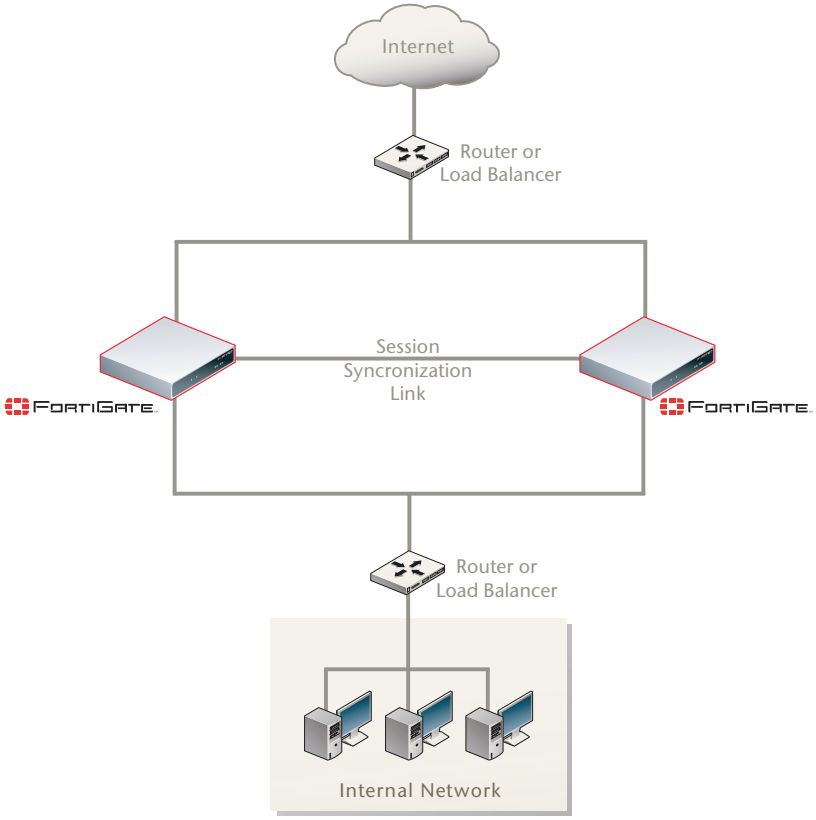
Use this command to configure TCP session synchronization between two standalone FortiGate units. You can use this feature with external routers or load balancers configured to distribute or load balance TCP sessions between two peer FortiGate units. If one of the peers fails, session failover occurs and active TCP sessions fail over to the peer that is still operating. This failover occurs without any loss of data. As well the external routers or load balancers will detect the failover and re-distribute all sessions to the peer that is still operating.

Note: TCP session synchronization between two standalone FortiGate units is also sometimes called standalone session synchronization or session synchronization between non-HA FortiGate units.

Note: You cannot configure standalone session synchronization when HA is enabled.

Standalone session synchronization can be used instead of HA to provide TCP session synchronization between two peer FortiGate units. If the external load balances direct all sessions to one peer the affect is similar to active-passive HA. If external load balancers or routers load balance traffic to both peers, the affect is similar to active-active HA. The load balancers should be configured so that all of the packets for any given session are processed by the same peer. This includes return packets.

Figure 6: Standalone session synchronization



By default, standalone session synchronization synchronizes all TCP sessions. You can optionally add filters to a configuration control which TCP sessions are synchronized. You can add filters to only synchronize packets from specified source and destination addresses, specified source and destination interfaces, and specified predefined firewall TCP services.

Unlike HA, standalone session synchronization does not include configuration synchronization. In fact, the configuration of the two peers is not identical because in most cases the peers would have different IP addresses. Also unlike HA, load balancing is done by external routers or load balancers. The FortiGate units only perform session synchronization and session failover.

Notes and limitations

Standalone session synchronization has the following limitations:

- Only TCP sessions accepted by firewall policies are synchronized. Due to their non-stateful nature, UDP and ICMP sessions don't need to be synchronized to naturally failover.
- Standalone session synchronization is a global configuration option. As a result you can only add one predefined firewall TCP service to a filter configuration. You cannot add custom services or service groups even if virtual domains are not enabled.
- You can only add one filter configuration to a given standalone session synchronization configuration. However, you can add multiple filters by adding multiple identical standalone session synchronization configurations, each one with a different filter configuration.
- Sessions accepted by firewall policies that contain protection profiles are not synchronized.
- Sessions that include network address translation (NAT) applied by selecting NAT in firewall policies are not synchronized because the address translation binds to a FortiGate unit address and the peers have different IP addresses.
- Session synchronization is a CLI only configuration.
- Session synchronization is available for FortiGate units or virtual domains operating in NAT/Route or Transparent mode. NAT sessions are not synchronized in either mode. In NAT/Route mode, only sessions for route mode firewall policies are synchronized. In Transparent mode, only sessions for normal Transparent mode policies are synchronized.
- Session synchronization cannot be asymmetric. Session synchronization is stateful. So all of the packets of a given session must be processed on the same peer. This includes return packets. You must configure the load balancers so that they do not cause asymmetric routing.
- Session synchronization is supported for traffic on physical interfaces, VLAN interfaces, zones, and aggregate interfaces. Session synchronization has not been tested for inter-vdom links, accelerated interfaces (FA2 and NP2), between HA clusters, and for redundant interfaces.
- The names of the matching interfaces, including VLAN interfaces, aggregate interfaces and so on, must be the same on both peers.

Configuring session synchronization

You configure session synchronization for each virtual domain to be synchronized. If virtual domain configuration is not enabled, you configure session synchronization for the root virtual domain. When virtual domain configuration is enabled and you have added virtual domains you configure session synchronization for each virtual domain to be synchronized. You don’t have to synchronize all of the virtual domains.

You must configure session synchronization on both peers. The session synchronization configurations of each peer should compliment the other. In fact you can manage and configure both peers as separate FortiGate units. Using FortiManager, you can manage both peers as two separate FortiGate devices.

On each peer, configuring session synchronization consists of selecting the virtual domains to be synchronized using the `syncvd` field, selecting the virtual domain on the other peer that receives the synchronization packets using the `peervd` field, and setting IP address of the interface in the peer unit that receives the synchronization packets using the `peerip` field. The interface with the `peerip` must be in the `peervd` virtual domain.

The `syncvd` and `peervd` settings must be the same on both peers. However, the `peerip` settings will be different because the `peerip` setting on the first peer includes the IP address of an interface on the second peer. And the `peerip` setting on the second peer includes the IP address of an interface on the first peer.

Because session synchronization does not synchronize FortiGate configuration settings you must configure both peers separately. For session synchronization to work properly all session synchronized virtual domains must be added to both peers. The names of the matching interfaces in each virtual domain must also be the same; this includes the names of matching VLAN interfaces. Note that the index numbers of the matching interfaces and VLAN interfaces can be different. Also the VLAN IDs of the matching VLAN interfaces can be different.

As well, the session synchronized virtual domains should have the same firewall policies so that sessions can be resumed after a failover using the same firewall policies.

For a configuration example, see "Basic example configuration" on page 513.

Configuring the session synchronization link

When session synchronization is operating, the peers share session information over an Ethernet link between the peers similar to an HA heartbeat link. Usually you would use the same interface on each peer for session synchronization. You should connect the session synchronization interfaces directly without using a switch or other networking equipment. If possible use a crossover cable for the session synchronization link. For FortiGate-5000 systems you can use a backplane interface as the session synchronization link.

You can use different interfaces on each peer for session synchronization links. Also, if you multiple sessions synchronization configurations, you can have multiple session synchronization links between the peers. In fact if you are synchronizing a lot of sessions, you may want to configure and connect multiple session synchronization links to distribute session synchronization traffic to these multiple links.

You cannot configure backup session synchronization links. Each configuration only includes one session synchronization link.

The session synchronization link should always be maintained. If session synchronization communication is interrupted and a failure occurs, sessions will not failover and data could be lost.

Session synchronization traffic can use a considerable amount of network bandwidth. If possible, session synchronization link interfaces should only be used for session synchronization traffic and not for data traffic.

Syntax

```
config system session-sync
  edit <sync_id>
    set peerip <peer_ipv4>
    set peervd <vd_name>
    set syncvd <vd_name>
    config filter
      set dstaddr <dist_ip_ipv4> <dist_mask_ipv4>
      set dstintf <interface_name>
      set service <string>
      set srcaddr <string>
      set srcintf <interface_name>
```

```
    end
  end
```

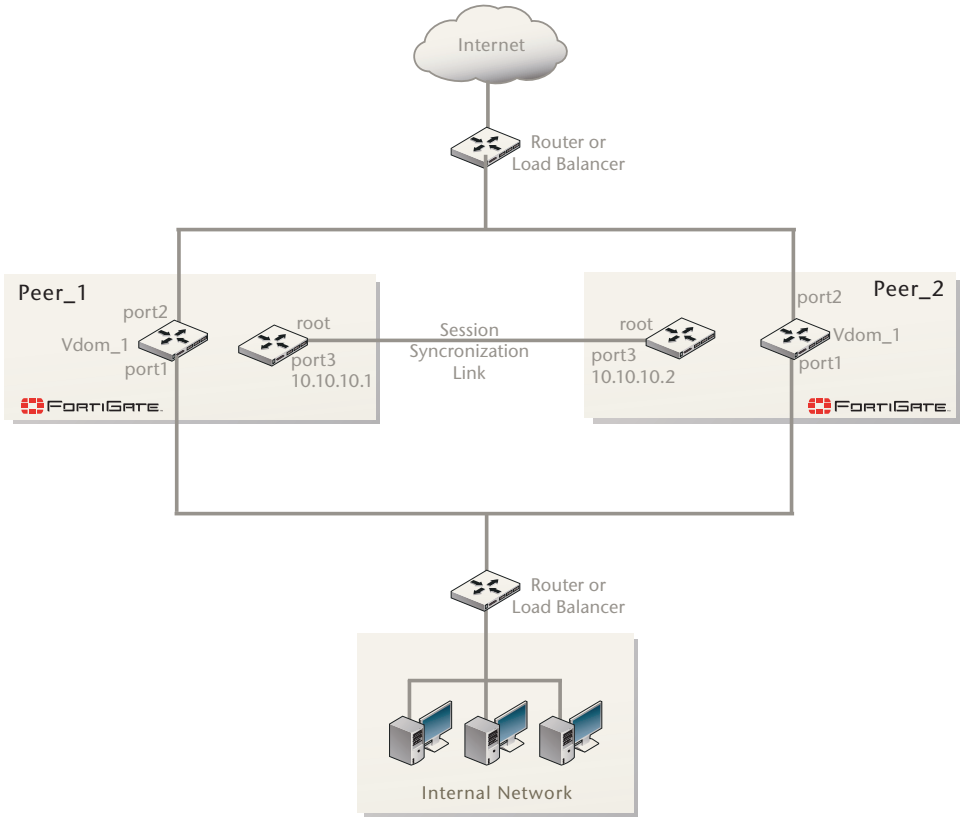
Variable	Description	Default
<sync_id>	Enter the unique ID number for the session synchronization configuration to edit. The session synchronization configuration ID can be any number between 1 and 200. The session synchronization configuration IDs of the peers do not have to match.	No default.
peerip <peer_ipv4>	Enter the IP address of the interface on the peer unit that is used for the session synchronization link.	0.0.0.0
peervd <vd_name>	Enter the name of the virtual domain that contains the session synchronization link interface on the peer unit. Usually both peers would have the same peervd. Multiple session synchronization configurations can use the same peervd.	root
syncvd <vd_name>	Enter the names of one or more virtual domains so that the sessions processed by these virtual domains are synchronized using this session synchronization configuration.	
config filter	Add a filter to a standalone session synchronization configuration. You can add a filter if you want to only synchronize some TCP sessions. Using a filter you can configure synchronization to only synchronize sessions according to source and destination address, source and destination interface, and predefined firewall TCP service. You can only add one filter to a standalone session synchronization configuration.	
dstaddr <dist_ip_ipv4> <dist_mask_ipv4>	Enter the destination IP address and netmask of the sessions to synchronize. You can use <dist_ip_ipv4> and <dist_mask_ipv4> to specify a single IP address or a range of IP addresses. The default IP address and netmask of 0.0.0.0 and 0.0.0.0 synchronizes sessions for all destination address. If you want to specify multiple IP addresses or address ranges you can add multiple standalone session synchronization configurations.	0.0.0.0 0.0.0.0
dstintf <interface_name>	Enter the name of a FortiGate interface (this can be any interface including a VLAN interface, aggregate interface, redundant interface, virtual SSL VPN interface, or inter-VDOM link interface). Only sessions destined for this interface are synchronized. You can only enter one interface name. If you want to synchronize sessions for multiple interfaces you can add multiple standalone session synchronization configurations. The default dstintf setting synchronizes sessions for all interfaces.	(null)
service <string>	Enter the name of a FortiGate firewall predefined service. Only sessions that use this predefined service are synchronized. You can only enter one predefined service name. If you want to synchronize sessions for multiple services you can add multiple standalone session synchronization configurations.	(null)
srcaddr <string>	Enter the source IP address and netmask of the sessions to synchronize. You can use <dist_ip_ipv4> and <dist_mask_ipv4> to specify a single IP address or a range of IP addresses. The default IP address and netmask of 0.0.0.0 and 0.0.0.0 synchronizes sessions for all source address. If you want to specify multiple IP addresses or address ranges you can add multiple standalone session synchronization configurations.	0.0.0.0 0.0.0.0
srcintf <interface_name>	Enter the name of a FortiGate interface (this can be any interface including a VLAN interface, aggregate interface, redundant interface, virtual SSL VPN interface, or inter-VDOM link interface). Only sessions from this interface are synchronized. You can only enter one interface name. If you want to synchronize sessions for multiple interfaces you can add multiple standalone session synchronization configurations. The default srcintf setting synchronizes sessions for all interfaces.	(null)

Basic example configuration

The following configuration example shows how to configure a basic session synchronization configuration for two peer FortiGate units shown in Figure 7 on page 513. The host names of peers are peer_1 and peer_2. Both peers are configured with two virtual domains: root and vdom_1. All sessions processed by vdom_1 are synchronized. The synchronization link interface is port3 which is in the root virtual domain. The IP address of port3 on peer_1 is 10.10.10.1. The IP address of port3 on peer_2 is 10.10.10.2.

Also on both peers, port1 and port2 are added to vdom_1. On peer_1 the IP address of port1 is set to 192.168.20.1 and the IP address of port2 is set to 172.110.20.1. On peer_2 the IP address of port1 is set to 192.168.20.2 and the IP address of port2 is set to 172.110.20.2.

Figure 7: Example standalone session synchronization network configuration



Configuration steps

1. Configure the load balancer or router to send all sessions to peer_1.
2. Configure the load balancer or router to send all traffic to peer_2 if peer_1 fails.
3. Use normal FortiGate configuration steps on peer_1:
   - Enable virtual domain configuration.
   - Add the vdom_1 virtual domain.
   - Add port1 and port2 to the vdom_1 virtual domain and configure these interfaces.
   - Set the IP address of port1 to 192.168.20.1.
   - Set the IP address of port2 to 172.110.20.1.
   - Set the IP address of port3 to 10.10.10.1.
   - Add route mode firewall policies between port1 and port2 to vdom_1.

4 Enter the following commands to configure session synchronization for peer_1

```
config system session-sync
  edit 1
    set peerip 10.10.10.2
    set peervd root
    set syncvd vdom_1
end
```

5 Use normal FortiGate configuration steps on peer_2:

- Enable virtual domain configuration.
- Add the vdom_1 virtual domain.
- Add port1 and port2 to the vdom_1 virtual domain and configure these interfaces.
- Set the IP address of port1 to 192.168.20.2.
- Set the IP address of port2 to 172.110.20.2.
- Set the IP address of port3 to 10.10.10.1.
- Add route mode firewall policies between port1 and port2 to vdom_1.

6 Enter the following commands to configure session synchronization for peer_1

```
config system session-sync
  edit 1
    set peerip 10.10.10.1
    set peervd root
    set syncvd vdom_1
end
```

Adding a filter

You can add a filter to this basic configuration if you only want to synchronize some TCP sessions. For example you can enter the following commands on both FortiGate units to edit the standalone sessions configurations and add a filter so that only HTTP sessions are synchronized

```
config system session-sync
  edit 1
    config filter
      set service HTTP
    end
end
```

History

FortiOS v3.0 MR6 The command `config system session-sync` is new for FortiOS v3.0 MR6.

FortiOS v3.0 MR7 The `config filter` command and associated fields (`dstaddr`, `dstintf`, `service`, `srcaddr`, and `srcintf`) are now available for MR7.

session-ttl

Use this command to configure port-range based session timeouts by setting the session time to live (ttl) for multiple TCP or UDP port number ranges. The session ttl is the length of time a TCP or UDP session can be idle before being dropped by the FortiGate unit. You can add multiple port number ranges. For each range you can configure the protocol (TCP or UDP) and start and end numbers of the port number range.

Syntax

```
config system session-ttl
  set default <seconds>
  config port
    edit <port_range_index>
      set end-port <port_number_int>
      set protocol <protocol_int>
      set start-port <port_number_int>
      set timeout {<timeout_int> | never}
    end
end
```

Variable	Description	Default
default <seconds>	Enter a the default session timeout in seconds. The valid range is from 300 - 604 800 seconds.	3600
<port_range_index>	Add a new port-number range.	No default.
end-port <port_number_int>	The end port number of the port number range. You must configure both the start-port and end-port. To specify a range, the start-port value must be lower than the end-port value. To specify a single port, the start-port value must be identical to the end-port value. The range is 0 to 65 535.	0
protocol <protocol_int>	Enter the protocol number to match the protocol of the sessions for which to configure a session ttl range. The Internet Protocol Number is found in the IP packet header. RFC 5237 describes protocol numbers and you can find a list of the assigned protocol numbers here. The range is from 0 to 255. To enter a port number range you must set protocol to 6 for TCP sessions or to 17 for UDP sessions.	0
start-port <port_number_int>	The start port number of the port number range. You must configure both the start-port and end-port. To specify a range, the start-port value must be lower than the end-port value. To specify a single port, the start-port value must be identical to the end-port value. The range is 0 to 65 535.	0
timeout {<timeout_int> | never}	Enter the number of seconds the session can be idle for on this port. The valid range is from 300 - 604800 seconds. Optionally you can enter never instead of specifying the number of seconds if you want the session to never expire. **Caution:** While it is possible to set timeout to never, this is not a secure configuration and should be avoided.	300

Examples

The following command increases the default session timeout:

```
config system session-ttl
  set default 62000
end
```

Use the following command to change the session timeout for TCP protocol SSH on port 22 to 3600 seconds.

```
config system session-ttl
  config port
  edit 1
    set protocol 6
    set start-port 22
    set end-port 22
    set timeout 3600
  end
end
```

History

FortiOS v2.80	Revised.
FortiOS v3.0	Changed from `session_ttl` to `session-ttl`.
FortiOS v3.0 MR3	Added `never` option to `timeout`, and added valid ranges for times for `timeout` and `default`.
FortiOS 4.0	Command changed to support multiple port-range based session ttl. The following fields added: `end-port`, `protocol`, and `start-port`.

settings

Use this command to change settings that are per VDOM settings such as the operating mode and default gateway.

When changing the opmode of the VDOM, there are fields that are visible depending on which opmode you are changing to. They are only visible after you set the opmode ab before you commit the changes with either ‘end or ‘next’. If you do not set these fields, the opmode change will fail.

Table 32: Fields associated with each opmode

Change from NAT to Transparent mode	Change from Transparent to NAT mode
`set gateway <gw_ipv4>`	`set device <interface_name>`
`set manageip <manage_ipv4>`	`set gateway <gw_ipv4>`
	`set ip <address_ipv4>`

`system settings` differs from `system global` in that `system global` fields apply to the entire FortiGate unit, where `system settings` fields apply only to the current VDOM, or the entire FortiGate unit if VDOMs are not enabled.

Bi-directional Forwarding Detection (BFD) is a protocol used by BGP and OSPF. It is used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and if a timer runs out on a connection then that router is declared down. BFD then communicates this information to the routing protocol and the routing information is updated. BFD support was added in FortiOS v3.0 MR4, and can only be configured through the CLI.

Syntax

```
config system settings
  set allow-subnet-overlap {enable | disable}
  set asymroute {enable | disable}
  set asymroute6 {enable | disable}
  set bfd {enable | disable}
  set bfd-desired-min-tx <interval_msec>
  set bfd-required-min-rx <interval_msec>
  set bfd-detect-mult <multiplier
  set bfd-dont-enforce-src-port {enable | disable}
  set comments <string>
  set device <interface_name>
  set ecmp-max-paths <max_entries>
  set gateway <gw_ipv4>
  set ip <address_ipv4>
  set manageip <manage_ipv4>
  set multicast-forward {enable | disable}
  set multicast-ttl-notchange {enable | disable}
  set opmode {nat | transparent}
  set sccp-port <port_number>
  set sip-helper {enable | disable}
  set sip-nat-trace {enable | disable}
  set sip-tcp-port <port_number>
  set sip-udp-port <port_number>
  set status {enable | disable}
  set strict-src-check {enable | disable}
  set utf8-spam-tagging {enable | disable}
  set vpn-stats-log {ipsec | l2tp | pptp | ssl}
  set vpn-stats-period <period_int>
```

```
end
```

Variable	Description	Default
`allow-subnet-overlap {enable | disable}`	Enable limited support for interface and VLAN subinterface IP address overlap for this VDOM. Use this command to enable limited support for overlapping IP addresses in an existing network configuration. Caution: for advanced users only. Use this only for existing network configurations that cannot be changed to eliminate IP address overlapping.	`disable`
`asymroute {enable | disable}`	Enable to turn on IPv4 asymmetric routing on your FortiGate unit, or this VDOM if you have VDOMs enabled. This feature should only be used as a temporary check to troubleshoot a network. It is not intended to be enabled permanently. When it enabled, many security features of your FortiGate unit are not enabled. For more information on asymmetric routing, see the FortiGate VLANs and VDOMs guide	`disable`
`asymroute6 {enable | disable}`	Enable to turn on IPv6 asymmetric routing on your FortiGate unit, or this VDOM if you have VDOMs enabled. This feature should only be used as a temporary check to troubleshoot a network. It is not intended to be enabled permanently. When it enabled, many security features of your FortiGate unit are not enabled. For more information on asymmetric routing, see the FortiGate VLANs and VDOMs guide	`disable`
`bfd {enable | disable}`	Enable to turn on bi-directional forwarding detection (BFD) for this virtual domain, or the whole FortiGate unit. BFD can be used with OSPF and BGP configurations, and overridden on a per interface basis.	`disable`
`bfd-desired-min-tx <interval_msec>`	Enter a value from 1 to 100 000 msec as the preferred minimum transmit interval for BFD packets. If possible this will be the minimum used. This variable is only available when bfd is enabled.	`50`
`bfd-required-min-rx <interval_msec>`	Enter a value from 1 to 100 000 msec as the required minimum receive interval for BFD packets. The FortiGate unit will not transmit BFD packets at a slower rate than this. This variable is only available when bfd is enabled.	`50`
`bfd-detect-mult <multiplier`	Enter a value from 1 to 50 for the BFD detection multiplier.	`3`
`bfd-dont-enforce-src-port {enable | disable}`	Enable to not enforce the BFD source port.	`disable`
`comments <string>`	Enter a descriptive comment for this virtual domain.	null
`device <interface_name>`	Enter the interface to use for management access. This is the interface to which `ip` applies. This field is visible only after you change `opmode` from `transparent` to `nat`, before you commit the change.	No default.
`ecmp-max-paths <max_entries>`	Enter the maximum number of routes allowed to be included in an Equal Cost Multi-Path (ECMP) configuration. Set to 1 to disable ECMP routing. ECMP routes have the same distance and the same priority, and can be used in load balancing.	10
`gateway <gw_ipv4>`	Enter the default gateway IP address. This field is visible only after you change `opmode` from `nat` to `transparent` or from `transparent` to `nat`, before you commit the change.	No default.
`ip <address_ipv4>`	Enter the IP address to use after switching to `nat` mode. This field is visible only after you change `opmode` from `transparent` to `nat`, before you commit the change.	No default.

Variable	Description	Default
`manageip <manage_ipv4>`	Set the IP address and netmask of the Transparent mode management interface. You must set this when you change `opmode` from `nat` to `transparent`. This option not available in transparent mode.	No default.
`multicast-forward {enable | disable}`	Enable or disable multicast forwarding to forward any multicast IP packets in which the TTL is 2 or higher to all interfaces and VLAN interfaces except the receiving interface. The TTL in the IP header will be reduced by 1. When multiple VDOMs are configured, this option is available within each VDOM.	`disable`
`multicast-ttl-notchange {enable | disable}`	Enable to alter multicast forwarding so that it does not decrement the time-to-live (TTL) in the packet header. Disable for normal multicast forwarding behavior. In multiple VDOM mode, this option is only available within VDOMs. It is not available at the global level.	`disable`
`opmode {nat | transparent}`	Enter the required operating mode. If you change `opmode` from `nat` to `transparent`, you must set `manageip` and `gateway`. If you change `opmode` from `transparent` to `nat`, you must set `device`, `ip`, `gateway-device` and `gateway`.	`nat`
`sccp-port <port_number>`	Enter the port number from 1 to 65535 of the TCP port to use to monitor Skinny Client Call protocol (SCCP) traffic. SCCP is a Cisco proprietary protocol for VoIP.	`2000`
`sip-helper {enable | disable}`	Enable to use the helper to add dynamic sip firewall allow rules.	`enable`
`sip-nat-trace {enable | disable}`	Select enable to record the original IP address of the phone.	`enable`
`sip-tcp-port <port_number>`	Enter a port number from 1 to 65535 for the TCP port the SIP proxy will use to monitor for SIP traffic.	`5060`
`sip-udp-port <port_number>`	Enter a port number from 1 to 65535 for the UDP port the SIP proxy will use to monitor for SIP traffic.	`5060`
`status {enable | disable}`	Disable or enable this VDOM. Disabled VDOMs keep all their configuration, but the resources of that VDOM are not accessible. To leave VDOM mode, all disabled VDOMs must be deleted - to leave VDOM mode there can be only the root VDOM configured. Only available when VDOMs are enabled.	`enable`
`strict-src-check {enable | disable}`	Enable to refuse packets from a source IP range if there is a specific route in the routing table for this network (RFC 3704).	`disable`
`utf8-spam-tagging {enable | disable}`	Enable converts spam tags to UTF8 for better non-ascii character support.	`enable`

Variable	Description	Default
`v4-ecmp-mode {source-ip-based | usage-based | weight-based}`	Set the ECMP route failover and load balance method, which controls how the FortiGate unit assigns a route to a session when multiple equal-cost routes to the sessions's destination are available. You can select: **`source-ip-based`** — the FortiGate unit load balances sessions among ECMP routes based on the source IP address of the sessions to be load balanced. No other settings can be configured to support source IP load balancing. **`weight-based`** — the FortiGate unit load balances sessions among ECMP routes based on weights added to ECMP routes. More traffic is directed to routes with higher weights. Use the `weight` field of the `config router static` command to add weights to static routes. See "router static" on page 361. **`usage-based`** — the FortiGate unit distributes sessions among ECMP routes based on how busy the FortiGate interfaces added to the routes are. After selecting `usage-based` you use the `spillover-threshold` field of the `config system interface` command to add spillover thresholds to interfaces added to ECMP routes. The FortiGate unit sends all ECMP-routed sessions to the lowest numbered interface until the bandwidth being processed by this interface reaches its spillover threshold. The FortiGate unit then spills additional sessions over to the next lowest numbered interface. See "system interface" on page 448.	`source-ip-based`
`vpn-stats-log {ipsec | l2tp | pptp | ssl}`	Enable periodic VPN log statistics for selected traffic: **`ipsec`** **`l2tp`** **`pptp`** **`ssl`**	
`vpn-stats-period <period_int>`	Enter the interval in seconds for `vpn-stats-log` to collect statistics.	0

Example

Changing the opmode from Transparent to NAT involves a number of steps. For example, before you change the opmode, the other required fields ip, device, and gateway are not visible.

This example changes to NAT opmode in a VDOM called vdom2. The management interface is set to internal, and the management IP is set to 192.168.10.8 with a gateway of 192.168.10.255.

```
config vdom
  edit vdom2
    config system settings
      set opmode nat
      set device internal
      set ip 192.168.10.8
      set gateway internal
    end
  end
```

History

FortiOS v3.0	New. `opmode` moved from `system global`. `manageip` moved from `system manageip`.
FortiOS v3.0 MR3	Added `multicast-forward` and `multicast-ttl-notchange`.

FortiOS v3.0 MR4	Added `asymroute`, `bfd`, `bfd-desired-min-tx`, `bfd-required-min-tx`, `bfd-detect-mult`, `bfd-dont-enforce-src-port`, `sccp-port`, `sip-helper`, `sip-tcp-port`, and `sip-udp-port`.
FortiOS v3.0 MR6	Added `comments`, `status`, `p2p-rate-limit`, `sip-nat-trace`, and `utf8-spam-tagging`. Removed `gateway-device`.
FortiOS v3.0 MR7	Added `allow-subnet-overlap`, `asymroute6`, and `strict-src-check` fields.
FortiOS v4.0	Added `vpn-stats-log` and `vpn-stats-period`. Removed `p2p-rate-limit`.
FortiOS 4.0 MR1	Added the `v4-ecmp-mode` field.

Related Commands

- vdom

sit-tunnel

Use this command to tunnel IPv6 traffic over an IPv4 network. The IPv6 interface is configured under `config system interface.` The command to do the reverse is `system ipv6-tunnel`.

Note: This command is not available in Transparent mode.

Syntax

```
config system sit-tunnel
  edit <tunnel_name>
    set destination <tunnel_address>
    set interface <name>
    set ip6 <address_ipv6>
    set source <address_ipv4>
  end
```

Variable	Description	Default
`edit <tunnel_name>`	Enter a name for the IPv6 tunnel.	No default.
`destination <tunnel_address>`	The destination IPv4 address for this tunnel.	0.0.0.0
`interface <name>`	The interface used to send and receive traffic for this tunnel.	No default.
`ip6 <address_ipv6>`	The IPv6 address for this tunnel.	No default.
`source <address_ipv4>`	The source IPv4 address for this tunnel.	0.0.0.0

Example

Use the following commands to set up an IPv6 tunnel.

```
config system sit-tunnel
  edit test_tunnel
    set destination 10.10.10.1
    set interface internal
    set ip6 12AB:0:0:CD30::/60
    set source 192.168.50.1
  end
```

History

FortiOS v2.80	New.
FortiOS v3.0	Changed from ipv6_tunnel to ipv6-tunnel.
FortiOS v3.0 MR1	Removed `vdom` field.
FortiOS v3.0 MR2	Added command syntax for multiple-vdom mode. Removed `ipv6` and `mode` fields.
FortiOS v3.0 MR5	Added `ip6`
FortiOS v3.0 MR7	Changed from `ipv6-tunnel` to `sit-tunnel`.

Related topics

- system interface
- system ipv6-tunnel

snmp community

Use this command to configure SNMP communities on your FortiGate unit. You add SNMP communities so that SNMP managers can connect to the FortiGate unit to view system information and receive SNMP traps. SNMP traps are triggered when system events happen such as when antivirus checking is bypassed, or when the log disk is almost full.

You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiGate unit for a different set of events. You can also the add IP addresses of up to 8 SNMP managers to each community.

For more information on SNMP traps and variables see the FortiGate Administration Guide, or the Fortinet Knowledge Center online.

Note: Part of configuring an SNMP manager is to list it as a host in a community on the FortiGate unit it will be monitoring. Otherwise the SNMP monitor will not receive any traps from that FortiGate unit, or be able to query it.

Syntax

```
config system snmp community
  edit <index_number>
    set events <events_list>
    set name <community_name>
    set query-v1-port <port_number>
    set query-v1-status {enable | disable}
    set query-v2c-port <port_number>
    set query-v2c-status {enable | disable}
    set status {enable | disable}
    set trap-v1-lport <port_number>
    set trap-v1-rport <port_number>
    set trap-v1-status {enable | disable}
    set trap-v2c-lport <port_number>
    set trap-v2c-rport <port_number>
    set trap-v2c-status {enable | disable}
    config hosts
    edit <host_number>
      set interface <if_name>
      set ip <address_ipv4>
    end
  end
```

Variable	Description	Default
`edit <index_number>`	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.	
`events <events_list>`	Enable the events for which the FortiGate unit should send traps to the SNMP managers in this community. **`amc-bypass`** — an AMC bridge module has switched to bridge (bypass) mode. **`av-bypass`** — FortiGate unit has entered bypass mode. See "`set av-failopen pass`" under "global" on page 423. **`av-conserve`** — System enters conserve mode. **`av-fragmented`** — A fragmented file has been detected. **`av-oversize`** — An oversized file has been detected. **`av-oversize-blocked`** — An oversized file has been blocked. **`av-oversize-passed`** — An oversized file has passed through. **`av-pattern`** — An file matching the AV pattern is detected. **`av-virus`** — A virus is detected. **`cpu-high`** — CPU usage exceeds threshold. Default is 80%. Automatic smoothing ensures only prolonged high CPU usage will trigger this trap, not a momentary spike. **`ent-conf-change`** — entity config change (rfc4133) **`faz-disconnect`** — A FortiAnalyzer device has disconnected from the FortiGate unit. **`fm-conf-change`** — FortiGate unit is managed by FortiManager, but the FortiGate administrator has modified the configuration directly. **`fm-if-change`** — FortiManager interface changes. **`ha-hb-failure`** — The HA heartbeat interface has failed. **`ha-member-down`** — The HA cluster member stops. **`ha-member-up`** — The HA cluster members starts. **`ha-switch`** — The primary unit in a HA cluster fails and is replaced with a new HA unit. **`intf-ip`** — The IP address of a FortiGate interface changes. **`ips-anomaly`** — IPS detects an anomaly. **`ips-pkg-update`** — IPS package has been updated. **`ips-signature`** — IPS detects an attack. **`log-full`** — Hard drive usage exceeds threshold. Default is 90%. **`mem-low`** — Memory usage exceeds threshold. Default is 80%. **`power-supply-failure`** — Power outage detected on monitored power supply. Available only on some models. **`vpn-tun-down`** — A VPN tunnel stops. **`vpn-tun-up`** — A VPN tunnel starts.	All events enabled.
`name <community_name>`	Enter the name of the SNMP community.	No default.
`query-v1-port <port_number>`	Enter the SNMP v1 query port number used for SNMP manager queries.	161
`query-v1-status {enable | disable}`	Enable or disable SNMP v1 queries for this SNMP community.	`enable`
`query-v2c-port <port_number>`	Enter the SNMP v2c query port number used for SNMP manager queries.	161
`query-v2c-status {enable | disable}`	Enable or disable SNMP v2c queries for this SNMP community.	`enable`
`status {enable | disable}`	Enable or disable the SNMP community.	`enable`
`trap-v1-lport <port_number>`	Enter the SNMP v1 local port number used for sending traps to the SNMP managers.	162
`trap-v1-rport <port_number>`	Enter the SNMP v1 remote port number used for sending traps to the SNMP managers.	162

Variable	Description	Default
trap-v1-status {enable | disable}	Enable or disable SNMP v1 traps for this SNMP community.	enable
trap-v2c-lport <port_number>	Enter the SNMP v2c local port number used for sending traps to the SNMP managers.	162
trap-v2c-rport <port_number>	Enter the SNMP v2c remote port number used for sending traps to the SNMP managers.	162
trap-v2c-status {enable | disable}	Enable or disable SNMP v2c traps for this SNMP community.	enable
hosts variables		
edit <host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.	
interface <if_name>	Enter the name of the FortiGate interface to which the SNMP manager connects.	No Default
ip <address_ipv4>	Enter the IP address of the SNMP manager.	0.0.0.0

Example

This example shows how to add a new SNMP community named SNMP_Com1. The default configuration can be used in most cases with only a few modifications. In the example below the community is added, given a name, and then because this community is for an SNMP manager that is SNMP v1 compatible, all v2c functionality is disabled. After the community is configured the SNMP manager is added. The SNMP manager IP address is 192.168.20.34 and it connects to the FortiGate unit internal interface.

```
config system snmp community
  edit 1
  set name SNMP_Com1
  set query-v2c-status disable
  set trap-v2c-status disable
    config hosts
      edit 1
      set interface internal
      set ip 192.168.10.34
      end
  end
```

History

FortiOS v2.80	Substantially revised.
FortiOS v2.80 MR6	fm_if_change added to events
FortiOS v3.0	Event names hyphens changed to underscores. Changed underscores to hyphens in field names.
FortiOS v3.0 MR3	New events added: av-fragmented, av-oversized, av-pattern, ha-hb-failure, temperature-high, and voltage-alarm. Added note.
FortiOS v3.0 MR7	Added event fields av-bypass, av-conserve, av-oversize-blocked, av-oversize-pass, ips-pkg-update, and power-supply-failure. Removed temperature-high and voltage-alert.

Related topics

- system snmp sysinfo

snmp sysinfo

Use this command to enable the FortiGate SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the FortiGate unit to identify it. When your SNMP manager receives traps from the FortiGate unit, you will know which unit sent the information. Some SNMP traps indicate high CPU usage, log full, or low memory.

For more information on SNMP traps and variables see the FortiGate Administration Guide, or the Fortinet Knowledge Center online.

Syntax

```
config system snmp sysinfo
  set contact-info <info_str>
  set description <description>
  set engine-id <engine-id_str>
  set location <location>
  set status {enable | disable}
  set trap-high-cpu-threshold <percentage>
  set trap-log-full-threshold <percentage>
  set trap-low-memory-threshold <percentage>
end
```

Variable	Description	Default
`contact-info <info_str>`	Add the contact information for the person responsible for this FortiGate unit. The contact information can be up to 35 characters long.	No default
`description <description>`	Add a name or description of the FortiGate unit. The description can be up to 35 characters long.	No default
`engine-id <engine-id_str>`	Each SNMP engine maintains a value, snmpEngineID, which uniquely identifies the SNMP engine. This value is included in each message sent to or from the SNMP engine. In FortiOS, the snmpEngineID is composed of two parts: • Fortinet prefix 0x8000304404 • the optional engine-id string, 24 characters maximum, defined in this command Optionally, enter an engine-id value.	No default
`location <location>`	Describe the physical location of the FortiGate unit. The system location description can be up to 35 characters long.	No default
`status {enable | disable}`	Enable or disable the FortiGate SNMP agent.	`disable`
`trap-high-cpu-threshold <percentage>`	Enter the percentage of CPU used that will trigger the threshold SNMP trap for the high-cpu. There is some smoothing of the high CPU trap to ensure the CPU usage is constant rather than a momentary spike. This feature prevents frequent and unnecessary traps.	80
`trap-log-full-threshold <percentage>`	Enter the percentage of disk space used that will trigger the threshold SNMP trap for the log-full.	90
`trap-low-memory-threshold <percentage>`	Enter the percentage of memory used that will be the threshold SNMP trap for the low-memory.	80

Example

This example shows how to enable the FortiGate SNMP agent and add basic SNMP information.

```
config system snmp sysinfo
  set status enable
  set contact-info 'System Admin ext 245'
```

```
    set description 'Internal network unit'
    set location 'Server Room A121'
  end
```

History

FortiOS v3.0	Changed `contact_info` to `contact-info`.
FortiOS v3.0 MR2	Added `trap-high-cpu-threshold`, `trap-log-full-threshold`, and `trap-low-memory-threshold` commands.
FortiOS v4.0	Revised.
FortiOS v4.0 MR1	Added `engine-id`.

Related topics

- system snmp community

snmp user

Use this command to configure an SNMP user including which SNMP events the user wants to be notified about, which hosts will be notified, and if queries are enabled which port to listen on for them.

FortiOS implements the user security model of RFC 3414. You can require the user to authenticate with a password and you can use encryption to protect the communication with the user.

For more information on SNMP traps and variables see the FortiGate Administration Guide, or the Fortinet Knowledge Center online.

Syntax

```
config system snmp user
  edit <username>
    set auth-proto {md5 | sha}
    set auth-pwd <password>
    set events <event_string>
    set notify-hosts <hosts_string>
    set priv-proto {aes | des}
    set priv-pwd <key>
    set queries {enable | disable}
    set query-port <port_int>
    set security-level <slevel>
  end
```

Variable	Description	Default
`edit <username>`	Edit or add selected user.	No default
`auth-proto {md5 | sha}`	Select authentication protocol: **md5** — use HMAC-MD5-96 authentication protocol. **sha** — use HMAC-SHA-96 authentication protocol. This is only available if `security-level` is `auth-priv` or `auth-no-priv`.	`sha`
`auth-pwd <password>`	Enter the user's password. Maximum 32 characters. This is only available if `security-level` is `auth-priv` or `auth-no-priv`.	No default.
`events <event_string>`	Select which SNMP notifications to send. Select each event that will generate a notification, and add to string. Separate multiple events by a space. Available events include: **amc-bypass** — an AMC bridge module has switched to bridge (bypass) mode. **av-bypass** — AV bypass happens **av-conserve** — AV system enters conserve mode **av-fragmented** — AV detected fragmented file **av-oversize** — AV detected oversized file **av-oversize-blocked** — AV oversized files blocked **av-oversize-passed** — AV oversized files passed **av-pattern** — AV detected file matching pattern **av-virus** — AV detected virus **cpu-high** — cpu usage too high **ent-conf-change** — entity config change (rfc4133) **faz-disconnect** — FortiAnalyzer unit disconnected **fm-conf-change** — config change (FM trap) **fm-if-change** — interface IP change (FM trap) **ha-hb-failure** — HA heartbeat interface failure **ha-member-down** — HA cluster member down **ha-member-up** — HA cluster member up	No default

Variable	Description	Default
events <event_string> (continued)	**ha-switch** — HA cluster status change **intf-ip** — interface IP address changed **ips-anomaly** — ips detected an anomaly **ips-pkg-update** — ips package updated **ips-signature** — ips detected an attack **log-full** — available log space is low **mem-low** — available memory is low **power-supply-failure** — power supply failure **vpn-tun-down** — VPN tunnel is down **vpn-tun-up** — VPN tunnel is up	
notify-hosts <hosts_string>	Enter IP address to send SNMP notifications (SNMP traps) to when events occur. Separate multiple addresses with a space.	No default
priv-proto {aes | des}	Select privacy (encryption) protocol: **aes** — use CFB128-AES-128 symmetric encryption. **des** — use CBC-DES symmetric encryption. This is available if security-level is auth-priv.	aes
priv-pwd <key>	Enter the privacy encryption key. Maximum 32 characters. This is available if security-level is auth-priv.	No default.
queries {enable | disable}	Enable or disable SNMP v3 queries for this user. Queries are used to determine the status of SNMP variables.	enable
query-port <port_int>	Enter the number of the port used for SNMP v3 queries. If multiple versions of SNMP are being supported, each version should listen on a different port.	161
security-level <slevel>	Set security level to one of: **no-auth-no-priv** — no authentication or privacy **auth-no-priv** — authentication but no privacy **auth-priv** — authentication and privacy	no-auth-no-priv

History

FortiOS v4.0 New.

FortiOS v4.0 MR1 Added auth-proto, auth-pwd, priv-proto, priv-pwd, and security-level.
Added amc-disconnect and faz-disconnect options to events field.

Related topics

- system snmp community, system snmp sysinfo

switch-interface

Use this command to group interfaces into a 'soft-switch' - a switch that is implemented in software instead of hardware. A group of switched interfaces have one IP address between them to connect to the FortiGate unit. This feature is available on all FortiGate models. For more information on switch-mode, see "global" on page 423.

Interfaces that may be members of a 'soft-switch' are physical and wlan interfaces that are not used anywhere else. Member interfaces cannot be monitored by HA or used as heart beat devices.

Syntax

```
config system switch-interface
  edit <group_name>
    set member <iflist>
    set span {enable | disable}
    set span-dest-port <portnum>
    set span-direction {rx | tx | both}
    set span-source-port <portlist>
    set type {hub | switch | hardware-switch}
    set vdom <vdom_name>
  end
```

Variable	Description	Default
<group_name>	The name for this group of interfaces. Cannot be in use by any other interfaces, vlans, or inter-VDOM links.	No default.
member <iflist>	Enter a list of the interfaces that will be part of this switch. Separate interface names with a space. Use <tab> to advance through the list of available interfaces.	No default.
span {enable | disable}	Enable or disable port spanning. This is available only when type is switch.	disable
span-dest-port <portnum>	Enter the destination port name. Use <tab> to advance through the list of available interfaces. Available when span is enabled.	No default.
span-direction {rx | tx | both}	Select the direction in which the span port operates: **rx** — Copy only received packets from source SPAN ports to the destination SPAN port. **tx** — Copy only transmitted packets from source SPAN ports to the destination SPAN port. **both** — Copy both transmitted and received packets from source SPAN ports to the destination SPAN port. span-direction is available only when span is enabled.	both
span-source-port <portlist>	Enter a list of the interfaces that are source ports. Separate interface names with a space. Use <tab> to advance through the list of available interfaces. Available when span is enabled.	No default.
type {hub | switch | hardware-switch}	Select the type of switch functionality: **hub** — duplicates packets to all member ports **switch** — normal switch functionality (available in NAT mode only) **hardware-switch** — unit electronics provides switch functionality **Note:** hardware-switch is available only on model 224B, where it is the only option for type.	switch
vdom <vdom_name>	Enter the VDOM to which the switch belongs.	No default.

Example

This example shows how to create a group of 3 interfaces called `low_speed` ideally that are all at 10m speed. It assumes these interfaces are not referred to in FortiOS by anything else.

```
config system switch-interface
  edit low_speed
    set member port1 wlan dmz
  end
```

History

FortiOS v3.0 MR6	New.
FortiOS v3.0 MR7	Added `span`, `span-dest-port`, `span-direction`, `span-source-port`, `type`, and `vdom` fields.
FortiOS v4.0	All models support this command.

tos-based-priority

Use this command to prioritize your network traffic based on its type-of-service (TOS).

IP datagrams have a TOS byte in the header (as described in RFC 791). Four bits within this field determine the delay, the throughput, the reliability, and cost (as described in RFC 1349) associated with that service. There are 4 other bits that are seldom used or reserved that are not included here. Together these bits are the tos variable of the tos-based-priority command.

The TOS information can be used to manage network traffic and its quality based on the needs of the application or service. TOS application routing (RFC 1583) is supported by OSPF routing.

For more information on TOS in routing, see "policy" on page 333.

Syntax

```
config system tos-based-priority
  edit <name>
    set tos <ip_tos_value>
    set priority [high | medium | low]
  end
```

Variable	Description	Default
`edit <name>`	Enter the name of the link object to create	No default.
`tos <ip_tos_value>`	Enter the value of the type of service byte in the IP datagram header. This value can be from 0 to 15.	0
`priority [high | medium | low]`	Select the priority of this type of service as either high, medium, or low priority. These priority levels conform to the firewall traffic shaping priorities.	`high`

Examples

It is a good idea to have your entry names in the tos-based-priority table and their TOS values be the same. Otherwise it can become confusing.

```
config tos-based-priority
  edit 1
    set tos 1
    set priority low
  next
  edit 4
    set tos 4
    set priority medium
  next
  edit 6
    set tos 6
    set priority high
  next
end
```

History

FortiOS v3.0 MR2 New command.

Related topics

- system global, router ospf, router policy, execute ping-options, ping6-options

vdom-link

Use this command to create an internal point-to-point interface object. This object is a link used to join virtual domains. Inter-VDOM links support BGP routing, and DHCP.

Creating the interface object also creates 2 new interface objects by the name of <name>0 and <name>1. For example if your object was named `v_link`, the 2 interface objects would be named `v_link0` and `v_link1`. You can then configure these new interfaces as you would any other virtual interface using `config system interface`.

When using vdom-links in HA, you can only have vdom-links in one vcluster. If you have vclusters defined, you must use the vcluster field to determine which vcluster will be allowed to contain the vdom-links.

Vdom-links support IPSec DHCP, but not regular DHCP.

A packet can pass through an inter-VDOM link a maximum of three times. This is to prevent a loop. When traffic is encrypted or decrypted it changes the content of the packets and this resets the inter-VDOM counter. However using IPIP or GRE tunnels do not reset the counter.

For more information on the vdom-link command see "Configuring inter-VDOM routing" on page 55 and the FortiGate VLANs and VDOMs Guide.

Syntax

```
config system vdom-link
  edit <name>
end
```

Variable	Description	Default
`edit <name>`	Enter the name of the link object to create. You are limited to 8 characters maximum for the name.	No default.
`vcluster {1|2}`	Select vcluster 1 or 2 as the only vcluster to have inter-VDOM links. This option is available only when HA and vclusters are configured, and there are VDOMs in both vclusters.	

Examples

In this example you have already created two virtual domains called v1 and v2. You want to set up a link between them. The following command creates the VDOM link called v12_link. Once you have the link you need to bind its two ends to the VDOMs it will be working with.

```
config system vdom-link
  edit v12_link
end

config system interface
  edit v12_link0
    set vdom v1
  next
  edit v12_link1
    set vdom v2
  end
```

If you want to delete the vdom-link, you must delete the interface - in the above example this would be:

```
config system interface
  delete v12_link
end
```

History

FortiOS v3.0	New command.
FortiOS v3.0 MR4	Added `vcluster` field.

Related topics

- router bgp
- system interface
- system dhcp server

vdom-property

Use this command to enter a description of a VDOM and to configure resource usage for the VDOM that overrides global limits and specifies guaranteed resource usage for the VDOM. When configuring resource usage for a VDOM you can set the *Maximum* and *Guaranteed* value for each resource.

- The Maximum value limits the amount of the resource that can be used by the VDOM. When you add a VDOM, all maximum resource usage settings are 0 indicating that resource limits for this VDOM are controlled by the global resource limits. You do not have to override the maximum settings unless you need to override global limits to further limit the resources available for the VDOM. You cannot set maximum resource usage higher in a VDOM than the corresponding global resource limit. For each resource you can override the global limit to reduce the amount of each resource available for this VDOM. The maximum must the same as or lower than the global limit. The default value is 0, which means the maximum is the same as the global limit.

Note: Use the command "system resource-limits" on page 506 to set global resource limits.

- The Guaranteed value represents the minimum amount of the resource available for that VDOM. Setting the guaranteed value makes sure that other VDOMs do not use all of a resource. A guaranteed value of 0 means that an amount of this resource is not guaranteed for this VDOM. You only have to change guaranteed settings if your FortiGate may become low on resources and you want to guarantee that a minimum level is available for this VDOM. For each resource you can enter the minimum amount of the resource available to this VDOM regardless of usage by other VDOMs. The default value is 0, which means that an amount of this resource is not guaranteed for this VDOM.

Syntax

```
config global
  config system vdom-property
    edit <vdom_name>
      set custom-service <max_int> [<guaranteed_int>]
      set description <description_str>
      set dialup-tunnel <max_int> [<guaranteed_int>]
      set firewall-policy <max_int> [<guaranteed_int>]
      set firewall-profile <max_int> [<guaranteed_int>]
      set firewall-address <max_int> [<guaranteed_int>]
      set firewall-addrgrp <max_int> [<guaranteed_int>]
      set ipsec-phase1 <max_int> [<guaranteed_int>]
      set ipsec-phase2 <max_int> [<guaranteed_int>]
      set onetime-schedule <max_int> [<guaranteed_int>]
      set recurring-schedule <max_int> [<guaranteed_int>]
      set service-group <max_int> [<guaranteed_int>]
      set session <max_int> [<guaranteed_int>]
      set user <max_int> [<guaranteed_int>]
      set user-group <max_int> [<guaranteed_int>]
    end
  end
```

Variable	Description	Default
`edit <vdom_name>`	Select the VDOM to set the limits for.	
`custom-service <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of firewall custom services.	0 0

Variable	Description	Default
`description <description_str>`	Enter a description of the VDOM. The description can be up to 63 characters long.	
`dialup-tunnel <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of dialup-tunnels.	0 0
`firewall-policy <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of firewall policies.	0 0
`firewall-profile <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of firewall profiles.	0 0
`firewall-address <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of firewall addresses.	0 0
`firewall-addrgrp <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of firewall address groups.	0 0
`ipsec-phase1 <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of IPSec phase1 tunnels.	0 0
`ipsec-phase2 <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of IPSec phase2 tunnels.	0 0
`onetime-schedule <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of onetime schedules.	0 0
`recurring-schedule <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of recurring schedules.	0 0
`service-group <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of firewall service groups.	0 0
`session <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of sessions.	0 0
`user <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of users.	0 0
`user-group <max_int> [<guaranteed_int>]`	Enter the maximum and guaranteed number of user groups.	0 0

Example

Use the following commands set a maximum of 500 sessions on the root VDOM with a guaranteed minimum level of 100 sessions. For this examples VDOMs are enabled.

```
config global
  config system vdom-property
    edit root
      set sesssion 500 100
    end
end
```

History

FortiOS v4.0 New.

Related topics

- system resource-limits

wccp

Configure settings for Web Cache Communication Protocol (WCCP) version 2 to optimize web traffic, thus reducing transmission costs and downloading time.

When a web client (on a computer) makes a request for web content, WCCP allows the routers on the local network to redirect the web content requests to the appropriate web cache server on the local network. If the web cache server contains the information in the web content request, the web cache server sends the content directly to the local client. If the web cache does not contain the requested information, the web cache server will download the HTTP information, cache it, and send it to the local client. The local client is not aware this caching is taking place.

For web caching to function, local network traffic must be directed through one or more routers that are able to forward the HTTP requests to the web cache servers. The FortiGate unit can act as a WCCP version 2 enabled router and direct web content requests to configured web cache servers.

The web caching will speed up downloads by not accessing remote websites for each HTTP request. It will also reduce the amount of data a company network sends and receives over the Internet, reducing costs.

```
config system wccp
  edit <service-id>
    set assignment-method {HASH | MASK | any}
    set authentication {disable | enable}
    set forward-method {GRE | L2 | any}
    set group-address <multicast_ipv4>
    set password <password_str>
    set return-method {GRE | L2 | any}
    set router-id <interface_ipv4>
    set server-list <server_ipv4mask>
  next
end
```

Variable	Description	Default
<service-id>	Valid ID range is from 0 to 255. 0 for HTTP.	1
assignment-method {HASH | MASK | any}	Specifies which assignment method the FortiGate unit prefers. If assignment-method is any the cache server determines the assignment method.	HASH
authentication {disable | enable}	Enable or disable using use MD5 authentication for the WCCP configuration.	disable
forward-method {GRE | L2 | any}	Specifies how the FortiGate unit forwards traffic to cache servers. If forward-method is any the cache server determines the forward method.	GRE
group-address <multicast_ipv4>	The IP multicast address used by the cache servers. 0.0.0.0 means the FortiGate unit ignores multicast WCCP traffic. Otherwise, group-address must be from 224.0.0.0 to 239.255.255.255.	0.0.0.0
password <password_str>	The authentication password. Maximum length is 8 characters.	No default.
return-method {GRE | L2 | any}	Specifies how a cache server declines a redirected packet and returns it to the FortiGate unit. If return-method is any the cache server determines the return method.	GRE

Variable	Description	Default
`router-id <interface_ipv4>`	An IP address known to all cache servers. This IP address identifies a FortiGate interface IP address to the cache servers. If all cache servers connect to the same FortiGate interface, then `<interface_ipv4>` can be `0.0.0.0`, and the FortiGate unit uses the IP address of that interface as the `router-id`. If the cache servers can connect to different FortiGate interfaces, you must set `router-id` to a single IP address, and this IP address must be added to the configuration of the cache servers.	`0.0.0.0`
`server-list <server_ipv4mask>`	The IP addresses of the web cache servers.	`0.0.0.0 0.0.0.0`

History

FortiOS v4.0 New.

wireless ap-status

On models that support Rogue Access Point Detection, you can use this command to designate access points as “accepted” or “rogue”. This designation affects the web-based manager Rogue AP listing.

You can use the `get system wireless detected-ap` command to obtain the required information. The FortiWiFi unit must be in SCAN mode or have `bg-scan` set to `enable`. For more information see “system wireless settings” on page 540.

Syntax

```
config system wireless ap-status
  edit <ap_id>
    set bssid <macaddr>
    set ssid <ssid>
    set status {accepted | rogue}
    end
```

Variable	Description	Default
`edit <ap_id>`	Enter a numeric identifier for this entry.	No default.
`bssid <macaddr>`	Enter MAC address of the access point.	No default.
`ssid <ssid>`	Enter the SSID of the access point.	No default.
`status {accepted | rogue}`	Set the designation of this access point: `accepted` — a known access point `rogue` — an unknown, possibly unsafe access point	`rogue`

History

FortiOS v4.0.0 New.

Related topics

- get system wireless detected-ap
- system wireless settings

wireless settings

Use this command to configure the WLAN interface wireless settings on a FortiWiFi unit.

Syntax

```
config system wireless settings
  set band {802.11a | 802.11b | 802.11g}
  set bgscan {enable | disable}
  set bgscan-idle <msec>
  set bgscan-interval <msec>
  set beacon_interval <integer>
  set channel <channel_number>
  set geography <Americas | EMEA | Israel | Japan | World>
  set mode <opmode>
  set power_level <dBm>
end
```

Except for `mode`, these fields are available in Access Point (AP) mode only.

Variable	Description	Default
`band {802.11a | 802.11b | 802.11g}`	Enter the wireless band to use. (802.11a only available on the FortiWiFi-60A and FortiWiFi-60B.)	802.11g
`bgscan {enable | disable}`	Enable scanning in the background. This provides scan mode capabilities in AP mode. When the AP channel is idle, the unit checks a scan channel and then returns to the AP channel. When the AP channel is idle again, the unit checks the next scan channel. This continues, repeatedly checking for signals on all wireless channels.	`disable`
`bgscan-idle <msec>`	Set how long in milliseconds the AP channel must be idle before the FortiWiFi unit checks a scan channel. Range 100 to 1000 ms. Higher values allow scanning only when wireless network traffic is light. Lower values allow more scanning, but this can cause packet loss in heavy network traffic. This is available only when `bgscan` is set to `enable`.	`250`
`bgscan-interval <msec>`	Set how long in milliseconds the FortiWiFi unit waits after scanning all wireless channels before beginning another cycle of scanning. This is available only when `bgscan` is set to `enable`.	`120`
`beacon_interval <integer>`	Set the interval between beacon packets. Access Points broadcast Beacons or Traffic Indication Messages (TIM) to synchronize wireless networks. In an environment with high interference, decreasing the Beacon Interval might improve network performance. In a location with few wireless nodes, you can increase this value. This is available in AP mode only.	`100`
`channel <channel_number>`	Select a channel number for your FortiWiFi unit wireless network. Use “0” to auto-select the channel. Users who want to use the wireless network should configure their computers to use this channel for wireless networking.	`5`
`geography <Americas | EMEA | Israel | Japan | World>`	Select the country or region in which this FortiWifi unit will operate.	`Americas`

Variable	Description	Default
`mode <opmode>`	Enter the operation mode for the wireless interface: **AP** — Access Point mode. Multiple wireless clients can connect to the unit. **CLIENT** — Connect to another wireless network as a client. **SCAN** — Scan all wireless bands and list the access points. ***Note***: When switching from AP mode to Client mode or Monitoring mode you must remove virtual wireless interfaces.	AP
`power_level <dBm>`	Set transmitter power level in dBm. Range 0 to 31. This is available in AP mode only.	17

Example

This example shows how to configure the wireless interface.

```
config system wireless settings
  set mode AP
  set channel 4
  set geography Americas
end
config system interface
  edit wlan
    set ip 10.10.80.1 255.255.255.0
    set wifi-ssid myssid
    set wifi-security WEP128
    set wifi-key ....
    ...
  end
end
```

History

FortiOS v2.80E	Command changed from `config system wireless wlan`. Fields added: `beacon_interval`, `broadcast_ssid`, `fragment_threshold`, `passphrase`, `power_level`, `radius_server`, `rts_threshold`
FortiOS v4.0.0	Removed `broadcast_ssid`, `fragment_threshold`, `key`, `passphrase`, `radius_server`, `rts_threshold`, `security`, `ssid`. Added fields `bgscan`, `bgscan-idle`, `bgscan-interval`.
FortiOS v4.1	Changed `geography` default to `Americas`.

Related topics

- system interface
- system vdom-link

zone

Use this command to add or edit zones.

In NAT/Route mode, you can group related interfaces or VLAN subinterfaces into zones. Grouping interfaces and subinterfaces into zones simplifies policy creation. For example, if you have two interfaces connected to the Internet, you can add both of these interfaces to the same zone. Then you can configure policies for connections to and from this zone, rather than to and from each interface.

In Transparent mode you can group related VLAN subinterfaces into zones and add these zones to virtual domains.

Syntax

```
config system zone
  edit <zone_name>
    set interface <name_str>
    set intrazone {allow | deny}
  end
```

Variable	Description	Default
`edit <zone_name>`	Enter the name of a new or existing zone.	
`interface <name_str>`	Add the specified interface to this zone. You cannot add an interface if it belongs to another zone or if firewall policies are defined for it.	No default.
`intrazone {allow | deny}`	Allow or deny traffic routing between different interfaces in the same zone.	`deny`

Example

This example shows how to add a zone named Zone1, add the internal interface to it, and to deny routing between different zones.

```
config system zone
  edit Zone1
    set interface internal
    set intrazone deny
  end
```

History

FortiOS v2.80 Revised.

FortiOS v2.80 MR2 `intrazone` now available on all models. All models support zones.
Added `interface` field (was part of `config system interface`).

Related topics

- system interface

user

This chapter covers:

- configuration of the FortiGate unit to use external authentication servers, including Windows Active Directory or other Directory Service servers
- configuration of user accounts and user groups for firewall policy authentication, administrator authentication and some types of VPN authentication
- configuration of peers and peer groups for IPSec VPN authentication and PKI user authentication

This chapter contains the following sections:

Configuring users for authentication

This chapter covers two types of user configuration:

- users authenticated by password
- users, sites or computers (peers) authenticated by certificate

Configuring users for password authentication

You need to set up authentication in the following order:

1 If external authentication is needed, configure the required servers.
   - See “user radius” on page 563.
   - See “user ldap” on page 555.
   - See “user tacacs+” on page 567
   - For Directory Service, see “user fsae” on page 549.

2 Configure local user identities.

   For each user, you can choose whether the FortiGate unit or an external authentication server verifies the password.
   - See “user local” on page 558.

3 Create user groups.

   Add local users to each user group as appropriate. You can also add an authentication server to a user group. In this case, all users in the server’s database can authenticate to the FortiGate unit.
   - See “user group” on page 551.
   - For Directory Service, also see “user ban” on page 545.

Configuring peers for certificate authentication

If your FortiGate unit will host IPSec VPNs that authenticate clients using certificates, you need to prepare for certificate authentication as follows:

1 Import the CA certificates for clients who authenticate with a FortiGate unit VPN using certificates.
   - See “vpn certificate ca” on page 570.

2 Enter the certificate information for each VPN client (peer).
   - See “user peer” on page 560.

3 Create peer groups, if you have VPNs that authenticate by peer group. Assign the appropriate peers to each peer group.
   - See “user peergrp” on page 562.

For detailed information about IPSec VPNs, see the *FortiGate IPSec VPN Guide*. For CLI-specific information about VPN configuration, see the VPN chapter of this Reference.

ban

The FortiGate unit compiles a list of all users, IP addresses, or interfaces that have a quarantine/ban rule applied to them. The Banned User list in the FortiGate web-based interface shows all IP addresses and interfaces blocked by NAC (Network Access Control) quarantine, and all IP addresses, authenticated users, senders and interfaces blocked by DLP (Data Leak Prevention). All users or IP addresses on the Banned User list are blocked until they are removed from the list, and all sessions to an interface on the list are blocked until the interface is removed from the list. Each banned user configuration can have an expiry time/date to automatically remove it from the Banned User list, or the user must be removed from the list manually by the system administrator.

Caution: You cannot configure items in the Banned user list with the CLI, you must use the web-based manager. In the CLI, you can display the list items in the Banned User list using `get user ban`, and remove items from the list using the following command:

```
config user ban
  delete banid <ban_int>
end
```

Syntax (view only, cannot be configured)

```
config user ban
edit banid <ban_int>
  set source {dlp-rule | dlp-compound | IPS | AV | DoS}
  set type {quarantine-src-ip | quarantine-dst-ip | quarantine-src-dst-ip
     | quarantine-intf | dlp-user | dlp-ip | dlp-sender | dlp-im}
  set cause {IPS (Intrusion Protection Sensor)) | Antivirus (AV) | Data
     Leak Prevention (DLP)}
  set src-ip-addr <src_ip_addr>
  set protocol {smtp | pop3 | imap | http-post | http-get | ftp-put |
     ftp-get | nntp | aim | icq | msn | ym | smtps | pop3s | imaps |
     https-post | https_get}
  set dst-ip-addr <dst_ip_addr>
  set interface <interface_name>
  set ip-addr <ip_addr>
  set user <user_name>
  set sender <sender_name>
  set im-type {aim | icq | msn | yahoo}
  set im-name <im_name>
  set expires <ban_expiry_date>
  set created <system_date>
 end
end
```

Variable	Description (or variable/description)	Default
`banid <ban_int>`	Enter the unique ID number of the banned user configuration. 0,0.	No default

Variable	Description (or variable/description)		Default
source {dlp-rule | dlp-compound | IPS | AV | DoS}	Enter one of the following to specify the source of the ban:		dlp-rule
	dlp-rule	Quarantine caused by a DLP rule configured by the system administrator.	
	dlp-compound	Quarantine caused by a DLP compound rule configured by the system administrator.	
	IPS	Quarantine caused by the FortiGate unit IPS.	
	AV	Quarantine caused by a virus detection by the FortiGate unit.	
	DoS	Quarantine caused by the DoS sensor.	
type {quarantine-src-ip | quarantine-dst-ip | quarantine-src-dst-ip | quarantine-intf | dlp-user | dlp-ip | dlp-sender | dlp-im}	Enter one of the following to specify the type of ban:		quarantine-src-ip
	quarantine-src-ip	Complete quarantine based on source IP address.	
	quarantine-dst-ip	Complete quarantine based on destination IP address.	
	quarantine-src-dst-ip	Block all traffic from source to destination address.	
	quarantine-intf	Block all traffic on the banned interface (port quarantine).	
	dlp-user	Ban based on user.	
	dlp-ip	Ban based on IP address of user.	
	dlp-sender	Ban based on email sender.	
	dlp-im	Ban based on IM user.	
cause {IPS (Intrusion Protection Sensor)) | Antivirus (AV) | Data Leak Prevention (DLP)}	Enter one of the following to specify the FortiGate function that caused the user, IP addresses or interfaces to be added to the Banned User list:		(null)
	IPS (Intrusion Protection Sensor)	Quarantine users or IP addresses that originate attacks detected by IPS.	
	Antivirus (AV)	Quarantine IP addresses or interfaces that send viruses detected by AV processing.	
	Data Leak Prevention (DLP)	Quarantine users or IP addresses that are banned or quarantined by DLP.	
src-ip-addr <src_ip_addr>	Enter the banned source IP address.		0.0.0.0

Variable	Description (or variable/description)		Default
protocol {smtp | pop3 | imap | http-post | http-get | ftp-put | ftp-get | nntp | aim | icq | msn | ym | smtps | pop3s | imaps | https-post | https_get}	Enter the protocol used by the user or IP addresses added to the Banned User list (ban type dlp-ip, dlp-sender, dlp-im, dlp-user).		No default
	smtp	smtp	
	pop3	pop3	
	imap	imap	
	http-post	http post	
	http-get	http get	
	ftp-put	ftp put	
	ftp-get	ftp get	
	nntp	nntp	
	aim	AOL instant messenger	
	icq	ICQ	
	msn	MSN messenger	
	ym	Yahoo! messenger	
	smtps	smtps	
	pop3s	pop3s	
	imaps	imaps	
	https-post	https post	
	https-get	https get	
dst-ip-addr <dst_ip_addr>	Enter the destination IP address to be quarantined/banned (ban type quarantine-dst-ip, quarantine-src-dst-ip).		
interface <interface_name>	Enter the interface to be quarantined/banned (ban type quarantine-intf). Available list of interfaces depends on FortiGate unit interface configuration.		null
	modem ()		
	interface1 ()		
	interface2 ()		
	interface3 ()		
	interface4 ()		
	interface5 ()		
	ssl.root ()		
ip-addr <ip_addr>	Enter the banned IP address (ban type dlp-ip)		0.0.0.0
user <user_name>	Enter the name of the user to be banned (ban type dlp-user).		null
sender <sender_name>	Enter the name of the sender to be banned (ban type dlp-sender).		null
im-type {aim | icq | msn | yahoo}	Enter the type of instant messenger to be banned (ban type dlp-im).		aim
	aim	AOL instant messenger	
	icq	ICQ	
	msn	MSN messenger	
	yahoo	Yahoo! messenger	
im-name <im_name>	Enter the name of the instant messenger to be banned (ban type dlp-im).		null

Variable	Description (or variable/description)	Default
`expires <ban_expiry_date>`	Specify when the ban is lifted by the FortiGate unit. Date and time `<yyyy/mm/dd hh:mm:ss>`. Range from 5 minutes to 365 days or `indefinite`. If set to `indefinite`, the ban must be manually removed from the Banned User list.	indefinite
`created <system_date>`	System-generated time that the ban was created by the system administrator. Format `Wed Dec 31 16:00:00 1969.`	No default

History

FortiOS v4.0 New. Banned User list items cannot be configured using the CLI.

Related topics

- user group
- firewall policy, policy6

fsae

Use this command to configure the FortiGate unit to receive user group information from a Directory Service server equipped with the Fortinet Server Authentication Extensions (FSAE). You can specify up to five computers on which a FSAE collector agent is installed. The FortiGate unit uses these collector agents in a redundant configuration. If the first agent fails, the FortiGate unit attempts to connect to the next agent in the list.

You can add user groups to Directory Service type user groups for authentication in firewall policies.

Syntax

```
config user fsae
  edit <server_name>
    set ldap_server <ldap-server-name>
    set password <password>
    set password2 <password2>
    set password3 <password3>
    set password4 <password4>
    set password5 <password5>
    set port <port_number>
    set port2 <port2_number>
    set port3 <por3_number>
    set port4 <port4_number>
    set port5 <port5_number>
    set server <domain>
    set server2 <domain2>
    set server3 <domain3>
    set server4 <domain4>
    set server5 <domain5>
  end
```

Variable	Description	Default
`edit <server_name>`	Enter a name to identify the Directory Service server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition.	No default.
`ldap_server <ldap-server-name>`	Enter the name of the LDAP server to be used to access the Directory Service.	No default.

`password <password>`
`password2 <password2>`
`password3 <password3>`
`password4 <password4>`
`password5 <password5>`
	For each collector agent, enter the password.	No default.

`port <port_number>`
`port2 <port2_number>`
`port3 <por3_number>`
`port4 <port4_number>`
`port5 <port5_number>`
	For each collector agent, enter the port number used for communication with FortiGate units.	`8000`

`server <domain>`
`server2 <domain2>`
`server3 <domain3>`
`server4 <domain4>`
`server5 <domain5>`
	Enter the domain name or IP address for up to five collector agents. Range from 1 to 63 characters.	No default.

History

FortiOS v3.0	New.
FortiOS v3.0 MR6	Added `ldap_server`, added range to `server <domain>`.
FortiOS v3.0 MR7	Changed Active Directory to Directory Service.

Related topics

- user group
- execute fsae refresh
- firewall policy, policy6

group

Use this command to add or edit user groups.

There are three types of user groups:

Firewall user group	Provides access to firewall policies that require authentication. A firewall policy specifies the user groups that are allowed to use the policy. Members of a firewall user group can be local users defined in `user local`, `peer members defined in user peer`, or accounts on RADIUS or LDAP servers configured in `user radius` or `user ldap`. Users must provide a user name and password to use the firewall policy.
SSL-VPN user group	Provides access to the FortiGate SSL-VPN tunnel and SSL-VPN web applications. Members of an SSL-VPN user group can be local users defined in `user local` or accounts on RADIUS or LDAP servers configured in `user radius` or `user ldap`. Users authenticate using their VPN client or through the SSL-VPN web portal login page.
Directory Service user group	Provides access to firewall policies that require authentication. Members of an Directory Service user group are members of selected Directory Service user groups on Directory Service servers configured in `user fsae`. Users are authenticated when they log on to their Windows domain and are not required to authenticate again to use FortiGate firewall policies.

To enable authentication, you must add user names, RADIUS servers and LDAP servers to one or more user groups. You can then select a user group when you require authentication. You can select a user group to configure authentication for:

- Firewall policies that require authentication

  Only users in the selected user group or users that can authenticate with the RADIUS or LDAP servers added to the user group can authenticate with these policies.
- SSL-VPN configurations
- IPSec VPN Phase 1 configurations for dialup users

  Only users in the selected user group can authenticate to use the VPN tunnel.
- XAuth for IPSec VPN Phase 1 configurations

  Only users in the selected user group can be authenticated using XAuth.
- FortiGate PPTP and L2TP configurations

  Only users in the selected user group can use the PPTP or L2TP configuration.
- Administrator login with RADIUS authentication

  If you use a user group for administrator authentication, it must contain only RADIUS servers.
- FortiGuard Web Filtering override groups

  When FortiGuard Web Filtering blocks a web page, authorized users can authenticate to access the web page or to allow members of another group to access it.

Note: User groups can utilize defined peer members as part of a group.

When you add user names, RADIUS servers, and LDAP servers to a user group, the order in which they are added determines the order in which the FortiGate unit checks for authentication. If user names are first, then the FortiGate unit checks first for a match with the local user names. If a match is not found, the FortiGate unit checks the RADIUS or LDAP server. If a RADIUS or LDAP server is added first, the FortiGate unit checks the server and then the local user names.

Syntax

```
config user group
  edit <groupname>
    set authtimeout <timeout>
    set group-type <grp_type>
    set ldap-memberof <LDAPgroup_str>
    set member <names>
    set profile <profilename>
    set sslvpn-portal <web_portal_name>
    set ftgd-wf-ovrd {allow | deny}
    set ftgd-wf-ovrd-dur <###d##h##m>
    set ftgd-wf-ovrd-dur-mode <mode>
    set ftgd-wf-ovrd-ext <option>
    set ftgd-wf-ovrd-profile <profile1 ... profilen>
    set ftgd-wf-ovrd-scope <scope>
    set ftgd-wf-ovrd-type <o_type>
end
```

Variable	Description	Default
`edit <groupname>`	Enter a new name to create a new group or enter an existing group name to edit that group.	No default.
`group-type <grp_type>`	Enter the group type. `<grp_type>` determines the type of users and is one of the following: • `directory-service` - Directory Service users • `firewall` - FortiGate users defined in user local, user ldap or user radius • `sslvpn` - SSL-VPN users	`firewall`
`ldap-memberof <LDAPgroup_str>`	Use this field if group members are authenticated by an LDAP server. Enter the LDAP groups to which members of this user group belong. `<LDAPgroup_str>` is an LDAP Distinguished Name (DN) specifying the group, for example `CN=group1,CN=Users,DC=test,DC=com`. You can specify multiple groups by separating the group DNs with a semicolon (;).	No default.
`member <names>`	Enter the names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Separate names by spaces. To add or remove names from the group you must re-enter the whole list with the additions or deletions required.	No default.
`profile <profilename>`	Enter the name of the firewall protection profile to associate with this user group. This is available if `group-type` is `firewall` or `directory-service`.	No default.
`authtimeout <timeout>`	Enter the value in seconds of an authentication timeout for the user group. If not set, global authentication timeout value used. 0 - 480 minutes. This is available if `group-type` is `firewall` or `directory-service`.	`0`
`sslvpn-portal <web_portal_name>`	Enter the name of the SSL-VPN portal for this group. This is available if `group-type` is `sslvpn`.	No default.
FortiGuard override variables	These are not available if `group-type` is `sslvpn`.	
`ftgd-wf-ovrd {allow | deny}`	Allow or deny this group FortiGuard Web Filtering overrides.	`deny`
`ftgd-wf-ovrd-dur <###d##h##m>`	Enter the FortiGuard Web Filtering override duration in days, hours, and minutes.	`15m`

Variable	Description	Default
ftgd-wf-ovrd-dur-mode <mode>	Enter the FortiGuard Web Filtering duration type, one of: • constant - as specified in ftgd-wf-ovrd-dur • ask - ask for duration when initiating override. ftgd-wf-ovrd-dur is the maximum	constant
ftgd-wf-ovrd-ext <option>	Enter one of the following to determine whether users can follow links to external sites during FortiGuard Web Filtering override: • allow • deny • ask	allow
ftgd-wf-ovrd-profile <profile1 ... profile*n*>	Enter the protection profiles that allow users of the firewall policy to override FortiGuard web filtering, regardless of their user group.	No default.
ftgd-wf-ovrd-scope <scope>	Enter the scope of the FortiGuard Web Filtering override, one of: user — override for the user user-group — override for the user's group ip — override for the initiating IP profile — override for the user's protection profile ask — ask for scope when initiating an override	user
ftgd-wf-ovrd-type <o_type>	Enter the type of FortiGuard Web Filtering override, one of: dir — override for the specific website directory domain — override for the specific domain rating — override for the specific rating ask — ask for type when initiating an override	dir

Example

This example shows how to add a group named User_Grp_1, and add User_2, User_3, Radius_2 and LDAP_1 as members of the group, and set the protection profile to strict:

```
config user group
    edit User_Grp_1
      set member User_2 User_3 Radius_2 LDAP_1
      set profile strict
  end
```

History

FortiOS v2.80	Revised.
FortiOS v2.80 MR3	Added profile field.
FortiOS v3.00 MR2	Expanded definition of sslvpn-client-check. Added field sslvpn-split-tunneling {enable | disable} Added field sslvpn-portal-heading <web_portal_string>.
FortiOS v3.00 MR3	Added field authtimeout. Added fields sslvpn-vnc and sslvpn-rdp.
FortiOS v3.00 MR4	Peer members can be included in user groups.
FortiOS v3.00 MR7	Added field sslvpn-ssh. Changed Active Directory to Directory Service. Added sslvpn-virtual-desktop, sslvpn-os-check, sslvpn-os-check-list, action, latest-patch-level, and tolerance.
FortiOS v4.0	Removed existing sslvpn fields. Added sslvpn-portal field. SSL VPN settings are now configured in vpn ssl web portal.
FortiOS v4.0 MR1	Added ldap-memberof field.

Related topics

- user ldap, user local, user radius, user tacacs+
- ssl web portal

ldap

Use this command to add or edit the definition of an LDAP server for user authentication.

To authenticate with the FortiGate unit, the user enters a user name and password. The FortiGate unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit. The maximum number of remote LDAP servers that can be configured for authentication is 10.

The FortiGate unit supports LDAP protocol functionality defined in RFC2251 for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3.

FortiGate LDAP support does not extend to proprietary functionality, such as notification of password expiration, that is available from some LDAP servers. FortiGate LDAP support does not supply information to the user about why authentication failed.

LDAP user authentication is supported for PPTP, L2TP, IPSec VPN, and firewall authentication. With PPTP, L2TP, and IPSec VPN, PAP (Packet Authentication Protocol) is supported and CHAP (Challenge Handshake Authentication Protocol) is not.

Syntax

```
config user ldap
  edit <server_name>
    set cnid <id>
    set dn <dname>
    set port <number>
    set server <domain>
    set type <auth_type>
    set username <ldap_username>
    set password <ldap_passwd>
    set group <group>
    set filter <group_filter>
    set secure <auth_port>
    set ca-cert <cert_name>
  end
```

Variable	Description	Default
`cnid <id>`	Enter the common name identifier for the LDAP server. The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid. Maximum 20 characters.	`cn`
`dn <dname>`	Enter the distinguished name used to look up entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the Common Name Identifier. The FortiGate unit passes this distinguished name unchanged to the server. You must provide a `dn` value if `type` is `simple`. Maximum 512 characters.	No default.
`edit <server_name>`	Enter a name to identify the LDAP server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition.	No default.
`port <number>`	Enter the port number for communication with the LDAP server.	`389`
`server <domain>`	Enter the LDAP server domain name or IP address.	No default.

Variable	Description	Default
type <auth_type>	Enter the authentication type for LDAP searches. One of: • anonymous - bind using anonymous user search • regular - bind using username/password and then search • simple - simple password authentication without search You can use simple authentication if the user records are all under one dn that you know. If the users are under more than one dn, use the anonymous or regular type, which can search the entire LDAP database for the required user name. If your LDAP server requires authentication to perform searches, use the regular type and provide values for username and password.	simple
username <ldap_username>	This field is available only if type is regular. For regular authentication, you need a user name and password. See your server administrator for more information.	No default.
password <ldap_passwd>	This field is available only if type is regular. For regular authentication, you need a user name and password. See your server administrator for more information.	No default.
group <group>	This field is available when the LDAP server must authenticate that a user is a member of this group on the LDAP server.	No default.
filter <group_filter>	Enter the name of the filter for group searches. The search for the group on the LDAP server is done with the following default filter configuration: (&(objectcategory=group)(member=*))	
secure <auth_port> {disable | starttls | ldaps}	Select the port to be used in authentication. disable — port 389 ldaps —port 636 starttls — port 389	disable
ca-cert <cert_name>	This field is available when secure is set to ldaps or starttls. User authentication will take place via a CA certificate. The CA certificate will be used by the LDAP library to validate the public certificate provided by the LDAP server.	null

Example

This example shows how to add an LDAP server called LDAP1 using the IP address 23.64.67.44, the default port, the common name cn, and the distinguished names ou=marketing,dc=fortinet,dc=com for simple authentication.

```
config user ldap
  edit LDAP1
    set server 23.64.67.44
    set cnid cn
    set dn ou=marketing,dc=fortinet,dc=com
  end
```

This example shows how to change the distinguished name in the example above to ou=accounts,ou=marketing,dc=fortinet,dc=com.

```
config user ldap
  edit LDAP1
    set dn ou=accounts,ou=marketing,dc=fortinet,dc=com
  end
```

History

FortiOS v2.80	Revised.
FortiOS v3.00 MR2	Added key word/variable `group <group>`.
FortiOS v3.00 MR3	Added fields `filter, secure, ca-cert.`
FortiOS v3.00 MR7	Maximum length for `dn` = 512 characters. Maximum length for `cnid` = 20 characters.

Related topics

- user group
- user local
- user radius
- user tacacs+

local

Use this command to add local user names and configure user authentication for the FortiGate unit. To add authentication by LDAP or RADIUS server you must first add servers using the `config user ldap` and `config user radius` commands.

Syntax

```
config user local
  edit <username>
    set ldap-server <servername>
    set passwd <password_str>
    set radius-server <servername>
    set status {enable | disable}
    set tacacs+-server <servername>
    set type <auth-type>
  end
```

Variable	Description	Default
`edit <username>`	Enter the user name. Enter a new name to create a new user account or enter an existing user name to edit that account.	
`ldap-server <servername>`	Enter the name of the LDAP server with which the user must authenticate. You can only select an LDAP server that has been added to the list of LDAP servers. See "ldap" on page 555. This is available when `type` is set to `ldap`.	No default.
`passwd <password_str>`	Enter the password with which the user must authenticate. Passwords at least 6 characters long provide better security than shorter passwords. This is available when `type` is set to `password`.	No default.
`radius-server <servername>`	Enter the name of the RADIUS server with which the user must authenticate. You can only select a RADIUS server that has been added to the list of RADIUS servers. See "radius" on page 563. This is available when `type` is set to `radius`.	No default.
`status {enable | disable}`	Enter `enable` to allow the local user to authenticate with the FortiGate unit.	`enable`
`tacacs+-server <servername>`	Enter the name of the TACACS+ server with which the user must authenticate. You can only select a TACACS+ server that has been added to the list of TACACS+ servers. See "tacacs+" on page 567. This is available when `type` is set to `tacacs+`.	No default.
`type <auth-type>`	Enter one of the following to specify how this user's password is verified: ldap — The LDAP server specified in `ldap-server` verifies the password. password — The FortiGate unit verifies the password against the value of `passwd`. radius — The RADIUS server specified in `radius-server` verifies the password. tacacs+ — The TACACS+ server specified in `tacacs+-server` verifies the password.	No default.

Example

This example shows how to add and enable a local user called Admin7 for authentication using the RADIUS server RAD1.

```
config user local
```

```
edit Admin7
  set status enable
  set type radius
  set radius-server RAD1
end
```

This example shows how to change the authentication method for the user Admin7 to password and enter the password.

```
config user local
  edit Admin7
    set type password
    set passwd abc123
  end
```

History

FortiOS v2.80	Revised.
FortiOS v2.80 MR2	Removed `try_other` field.

Related topics

- user group
- user ldap
- user radius
- user tacacs+

peer

Use this command to add or edit peer (digital certificate holder) information. You use the peers you define here in the `config vpn ipsec phase1` command if you specify `peertype` as `peer`. Also, you can add these peers to peer groups you define in the `config user peergrp` command.

For PKI user authentication, you can add or edit peer information and configure use of LDAP server to check access rights for client certificates.

This command refers to certificates imported into the FortiGate unit. You import CA certificates using the `vpn certificate ca` command. You import local certificates using the `vpn certificate local` command.

You can configure a peer user with no values in `subject` or `ca`. This user behaves like a user account or policy that is disabled.

Note: If you create a PKI user in the CLI with no values in `subject` or `ca`, you cannot open the user record in the GUI, or you will be prompted to add a value in Subject (`subject`) or CA (`ca`).

Syntax

```
config user peer
  edit <peer_name>
    set ca <ca_name>
    set cn <cn_name>
    set cn-type <type>
    set ldap-password <ldap_password>
    set ldap-server <ldap_server>
    set ldap-username <ldap_user>
    set mandatory-ca-verify {enable | disable}
    set passwd <password_str>
    set subject <constraints>
    set two-factor {enable | disable}
  end
```

Variable	Description	Default
`ca <ca_name>`	Enter the CA certificate name, as returned by `execute vpn certificate ca list`.	No default.
`cn <cn_name>`	Enter the peer certificate common name.	No default.
`cn-type <type>`	Enter the peer certificate common name type: `FQDN` — Fully-qualified domain name. `email` — The user's email address. `ipv4` — The user's IP address (IPv4). `ipv6` — The user's IP address (IPv6). `string` — Any other piece of information.	`string`
`edit <peer_name>`	Enter the peer name. Enter a new name to create a new peer or enter an existing peer name to edit that peer's information.	
`ldap-password <ldap_password>`	Enter the login password for the LDAP server used to perform client access rights check for the defined peer.	No default.
`ldap-server <ldap_server>`	Enter the name of one of the LDAP servers defined under 'config user ldap' used to perform client access rights check for the defined peer.	null
`ldap-username <ldap_user>`	Enter the login name for the LDAP server used to perform client access rights check for the defined peer.	null

Variable	Description	Default
`mandatory-ca-verify {enable | disable}`	If the CA certificate is installed on the FortiGate unit, the peer certificate is checked for validity. The `mandatory-ca-verify` field determines what to do if the CA certificate is not installed: **`enable`** — The peer cannot be authenticated. **`disable`** — The peer certificate is automatically considered valid and authentication succeeds.	`disable`
`passwd <password_str>`	Enter the password that this peer uses for two-factor authentication. The is available when `two-factor` is enabled.	No default.
`subject <constraints>`	Optionally, enter any of the peer certificate name constraints.	No default.
`two-factor {enable | disable}`	Enable user to authenticate by password in addition to certificate authentication. Specify the password in `passwd`.	`disable`

Example

This example shows how to add the `branch_office` peer.

Configure the peer using the CA certificate name and peer information:

```
config user peer
  edit branch_office
    set ca CA_Cert_1
    set cn ouraddress@example2.com
    set cn-type email
  end
```

Configure the peer with empty subject and ca fields.

```
config user peer
  edit peer2
end
```

History

FortiOS v2.80 MR2	New.
FortiOS v3.0 MR4	Addition of `ldap-password, ldap-server, ldap-username` for use of LDAP servers for PKI user authentication.
FortiOS v3.0 MR5	Addition of `cn-type <type> ipv6` for authentication of IPv6 IPSec.
FortiOS v3.0 MR6	Added description of empty `subject` and `ca` fields.
FortiOS v4.0	Added `mandatory-ca-verify`.
FortiOS v4.0 MR1	Added `password` and `two-factor`.

Related topics

- user peergrp
- vpn ipsec phase1
- vpn certificate ca
- vpn certificate local

peergrp

Use this command to add or edit a peer group. Peers are digital certificate holders defined using the `config user peer` command. You use the peer groups you define here in the `config vpn ipsec phase1` command if you specify `peertype` as `peergrp`.

For PKI user authentication, you can add or edit peer group member information. User groups that use PKI authentication can also be configured using `config user group`.

Syntax

```
config user peergrp
  edit <groupname>
    set member <peer_names>
  end
```

Variable	Description	Default
`edit <groupname>`	Enter a new name to create a new peer group or enter an existing group name to edit that group.	
`member <peer_names>`	Enter the names of peers to add to the peer group. Separate names by spaces. To add or remove names from the group you must re-enter the whole list with the additions or deletions required.	No default.

Example

This example shows how to add peers to the peergrp `EU_branches`.

```
config user peergrp
  edit EU_branches
    set member Sophia_branch Valencia_branch Cardiff_branch
  end
```

History

FortiOS v2.80 MR2 New.

Related topics

- user peer
- vpn ipsec phase1
- vpn l2tp
- vpn pptp

radius

Use this command to add or edit the information used for RADIUS authentication.

The default port for RADIUS traffic is 1812. If your RADIUS server is using a different port you can change the default RADIUS port. You may set a different port for each of your RADIUS servers. The maximum number of remote RADIUS servers that can be configured for authentication is 10.

The RADIUS server is now provided with more information to make authentication decisions, based on values in `server, use-management-vdom, use-group-for-profile, and nas-ip`. Attributes include:

- `NAS-IP-Address` - RADIUS setting or IP address of FortiGate interface used to talk to RADIUS server, if not configured
- `NAS-Port` - physical interface number of the traffic that triggered the authentication
- `Called-Station-ID` - same value as NAS-IP Address but in text format
- `Fortinet-Vdom-Name` - name of VDOM of the traffic that triggered the authentication
- `NAS-Identifier` - configured hostname in non-HA mode; HA cluster group name in HA mode
- `Acct-Session-ID` - unique ID identifying the authentication session
- `Connect-Info` - identifies the service for which the authentication is being performed (web-auth, vpn-ipsec, vpn-pptp, vpn-l2tp, vpn-ssl, admin-login, test)

You may select an alternative authentication method for each server. These include CHAP, PAP, MS-CHAP, and MS-CHAP-v2.

Syntax

```
config user radius
  edit <server_name>
    set all-usergroup {enable | disable}
    set auth-type {auto | chap | ms_chap | ms_chap_v2 | pap}
    set nas-ip <use_ip>
    set radius-port <radius_port_num>
    set secondary-secret <sec_server_password>
    set secondary-server <sec_server_domain>
    set secret <server_password>
    set server <domain>
    set use-group-for-profile {enable | disable}
    set use-management-vdom {enable | disable}
  end
```

Variable	Description	Default
`edit <server_name>`	Enter a name to identify the RADIUS server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition.	
`all-usergroup {enable | disable}`	Enable to automatically include this RADIUS server in all user groups.	disable
`auth-type {auto | chap | ms_chap | ms_chap_v2 | pap}`	Select the authentication method for this RADIUS server. `auto` uses `pap, ms_chap_v2, and chap.`	auto
`nas-ip <use_ip>`	IP address used as `NAS-IP-Address` and `Called-Station-ID` attribute in RADIUS access requests. RADIUS setting or IP address of FGT interface used to talk with RADIUS server, if not configured.	No default.

Variable	Description	Default
`radius-port <radius_port_num>`	Change the default RADIUS port for this server. The default port for RADIUS traffic is `1812`. Range is `0..65535`.	1812
`secondary-secret <sec_server_password>`	Enter the secondary RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length.	No default.
`secondary-server <sec_server_domain>`	Enter the secondary RADIUS server domain name or IP address.	No default.
`secret <server_password>`	Enter the RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length.	No default.
`server <domain>`	Enter the RADIUS server domain name or IP address.	No default.
`use-management-vdom {enable | disable}`	Enable to use the management VDOM to send all RADIUS requests.	disable
`use-group-for-profile {enable | disable}`	Enable to use RADIUS group attribute to select the protection profile.	disable

Example

This example shows how to add the radius server `RAD1` at the IP address `206.205.204.203` and set the shared secret as `R1a2D3i4U5s`.

```
config user radius
  edit RAD1
    set secret R1a2D3i4U5s
    set server 206.205.204.203
  end
```

History

FortiOS v2.80 Revised.

FortiOS v3.0 MR3 Added `use-management-vdom`, `use-group-for-profile`, nas-ip. Description of additional authentication attributes.

FortiOS v3.0 MR4 Added `secondary-server` and `secondary-secret`.

FortiOS v3.0 MR5 Added `all-usergroup`.

FortiOS v3.0 MR6 Added `auth-type {auto | chap | ms_chap | ms_chap_v2 | pap}`, and `radius-port`.

Related topics

- user group
- user ldap
- user local
- user tacacs+

setting

Use this command to change per VDOM user settings such as the firewall user authentication time out and protocol support for firewall policy authentication.

`user settings` differ from `system global settings` in that `system global settings` fields apply to the entire FortiGate unit, where `user settings` fields apply only to the user VDOM.

Syntax

```
config user setting
  set auth-blackout-time <blackout_time_int>
  set auth-cert <cert_name>
  set auth-http-basic {disable | enable}
  set auth-secure-http {enable | disable}
  set auth-type {ftp | http | https | telnet}
  set auth-timeout <auth_timeout_minutes>
  config auth-ports
    edit <auth-table-entry-id>
      set port <port_int>
      set type {ftp | http | https | telnet}
    end
end
```

Variable	Description	Default
`auth-blackout-time <blackout_time_int>`	When a firewall authentication attempt fails 5 times within one minute the IP address that is the source of the authentication attempts is denied access for the `<blackout_time_int>` period in seconds. The range is 0 to 3600 seconds.	`0`
`auth-cert <cert_name>`	HTTPS server certificate for policy authentication. Fortinet_Factory, Fortinet_Firmware (if applicable to your FortiGate unit), and self-sign are built-in certificates but others will be listed as you add them.	`self-sign`
`auth-http-basic {disable | enable}`	Enable or disable support for HTTP basic authentication for identity-based firewall policies. HTTP basic authentication usually causes a browser to display a pop-up authentication window instead of displaying an authentication web page. Some basic web browsers, for example, web browsers on mobile devices, may only support HTTP basic authentication.	`disable`
`auth-secure-http {enable | disable}`	Enable to have `http` user authentication redirected to secure channel - `https`.	`disable`
`auth-type {ftp | http | https | telnet}`	Set the user authentication protocol support for firewall policy authentication. User controls which protocols should support the authentication challenge.	
`auth-timeout <auth_timeout_minutes>`	Set the number of minutes before the firewall user authentication timeout requires the user to authenticate again. The maximum `authtimeout` interval is 480 minutes (8 hours). To improve security, keep the authentication timeout at the default value of 5 minutes.	`5`
`config auth-ports` **variables**		
`<auth-table-entry-id>`	Create an entry in the authentication port table if you are using non-standard ports.	
`port <port_int>`	Specify the authentication port. Range 1 to 65535.	`1024`
`type {ftp | http | https | telnet}`	Specify the protocol to which `port` applies.	`http`

Example

This example shows how to enable https user authentication, and set the firewall user authentication timeout to 15 minutes.

```
config user setting
  set auth-type https
  set auth-timeout 15
end
```

History

FortiOS v3.0 MR6	New. Replaces `system global variables authtimeout, auth-type, and auth-secure-http`
FortiOS 4.0 MR1	Added `auth-blackout-time` and `auth-http-basic`.

tacacs+

Use this command to add or edit the information used for TACACS+ authentication.

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol used to communicate with an authentication server. TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user.

The default port for a TACACS+ server is 49. The maximum number of remote TACACS+ servers that can be configured for authentication is 10.

You may select an alternative authentication method for each server. These include CHAP, PAP, MS-CHAP, and ASCII.

Syntax

```
config user tacacs+
  edit <server_name>
    set authen-type {ascii | auto | chap | ms_chap | pap}
    set key <server_key>
    set port <tacacs+_port_num>
    set server <domain>
  end
```

Variable	Description	Default
`edit <server_name>`	Enter a name to identify the TACACS+ server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition.	
`authen-type {ascii | auto | chap | ms_chap | pap}`	Select the authentication method for this TACACS+ server. `auto` uses `pap`, `ms_chap_v`, and `chap`, in that order.	auto
`key <server_key>`	Enter the key to access the server. The maximum number is 16.	
`port <tacacs+_port_num>`	Change the default TACACS+ port for this server. The default port for TACACS+ traffic is 49. Range is `0..65535`.	49
`server <domain>`	Enter the TACACS+ server domain name or IP address.	No default.

Example

This example shows how to add the TACACS+ server `TACACS1` at the IP address `206.205.204.203`, set the server key as `R1a2D3i4U5s, and authenticate using PAP`.

```
config user tacacs+
  edit TACACS1
    set authen-type pap
    set key R1a2D3i4U5s
    set server 206.205.204.203
  end
```

History

FortiOS v3.0 MR6 New.

Related topics

- user group, user local
- user ldap, user radius

vpn

Use vpn commands to configure options related to virtual private networking through the FortiGate unit, including:

- IPSec operating parameters
- a local address range for PPTP or L2TP clients
- SSL VPN configuration settings

This chapter contains the following sections:

certificate ca

Use this command to install Certificate Authority (CA) root certificates.

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute vpn certificate local` command to generate a CSR.
2. Send the CSR to a CA.

   The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `vpn certificate local` command to install the signed local certificate.
4. Use the `vpn certificate ca` command to install the CA certificate.
5. Use the `vpn certificate crl` command to install the CRL.

Depending on your terminal software, you can copy the certificate and paste it into the command.

The CA certificate can update automatically from a Simple Certificate Enrollment Protocol (SCEP) server.

Syntax

```
config vpn certificate ca
  edit <ca_name>
    set ca <cert>
    set auto-update-days <days_int>
    set auto-update-days-warning <days_int>
    set scep-url <URL_str>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get vpn certificate ca <ca_name>
```

Variable	Description	Default
`edit <ca_name>`	Enter a name for the CA certificate.	No default.
`ca <cert>`	Enter or retrieve the CA certificate in PEM format.	No default.
Fields relevant to SCEP auto-update		
`auto-update-days <days_int>`	Enter how many days before expiry the FortiGate unit requests an updated CA certificate. Enter `0` for no auto-update.	`0`
`auto-update-days-warning <days_int>`	Enter how many days before CA certificate expiry the FortiGate generates a warning message. Enter 0 for no warning.	`0`
`scep-url <URL_str>`	Enter the URL of the SCEP server.	No default.

History

FortiOS v3.0 New.

FortiOS v4.0 MR1 Added `auto-update-days`, `auto-update-days-warning`, and `scep-url`.

Related topics

- vpn certificate crl
- vpn certificate local
- vpn certificate ocsp
- vpn certificate remote
- execute vpn certificate ca

certificate crl

Use this command to install a Certificate Revocation List (CRL).

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute vpn certificate local` command to generate a CSR.
2. Send the CSR to a CA.

   The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `vpn certificate local` command to install the signed local certificate.
4. Use the `vpn certificate ca` command to install the CA certificate.
5. Use the `vpn certificate crl` command to install the CRL.

Depending on your terminal software, you can copy the certificate and paste it into the command.

The CRL can update automatically from a Simple Certificate Enrollment Protocol (SCEP) server.

Syntax

```
config vpn certificate crl
  edit <crl_name>
    set crl <crl_PEM>
    set ldap-server <ldap_server_name>
    set ldap-username <ldap_username>
    set ldap-password <ldap_password>
    set scep-cert <scep_certificate>
    set scep-url <scep_url>
    set update-vdom <update_vdom>
    set http-url <http_url>
    set update-interval <seconds>
  end
```

Variable	Description
`edit <crl_name>`	Enter a name for the Certificate Revocation List (CRL).
`crl <crl_PEM>`	Enter the CRL in PEM format.
`ldap-server <ldap_server_name>`	Name of the LDAP server defined in config user ldap table for CRL auto-update.
`ldap-username <ldap_username>`	LDAP login name.
`ldap-password <ldap_password>`	LDAP login password.
`scep-cert <scep_certificate>`	Local certificate used for SCEP communication for CRL auto-update.
`scep-url <scep_url>`	URL of the SCEP server used for automatic CRL certificate updates. Start with http://.
`update-vdom <update_vdom>`	VDOM used to communicate with remote SCEP server for CRL auto-update.

Variable	Description
`http-url <http_url>`	URL of an http server used for automatic CRL certificate updates. Start with http://.
`update-interval <seconds>`	Enter how frequently, in seconds, the FortiGate unit checks for an updated CRL. Enter `0` to update the CRL only when it expires.

History

FortiOS v3.0 New.

FortiOS v3.0 MR4 Added variables for use with certificate authentication (automatic CRL updates).

FortiOS v4.0 MR1 Added `update-interval`.

Related topics

- vpn certificate ca
- vpn certificate local
- vpn certificate ocsp
- vpn certificate remote
- execute vpn certificate crl

certificate local

Use this command to install local certificates.

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute vpn certificate local` command to generate a CSR.
2. Send the CSR to a CA.

   The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `vpn certificate local` command to install the signed local certificate.
4. Use the `vpn certificate ca` command to install the CA certificate.
5. Use the `vpn certificate crl` command to install the CRL.

Depending on your terminal software, you can copy the certificate and paste it into the command.

The local certificate can update automatically from a Simple Certificate Enrollment Protocol (SCEP) server.

Syntax

```
config vpn certificate local
  edit <cert_name>
    set password <pwd>
    set comments <comment_text>
    set private-key <prkey>
    set certificate <cert_PEM>
    set csr <csr_PEM>
    set scep-url <URL_str>
    set scep-password <password_str>
    set auto-regenerate-days <days_int>
    set auto-regenerate-days-warning <days_int>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get vpn certificate local [cert_name]
```

Variable	Description	Default
`edit <cert_name>`	Enter the local certificate name.	No default.
`certificate <cert_PEM>`	Enter the signed local certificate in PEM format.	No default.
`comments <comment_text>`	Enter any relevant information about the certificate.	No default.
You should not modify the following variables if you generated the CSR on this unit.		
`csr <csr_PEM>`	The CSR in PEM format.	No default.
`password <pwd>`	The password in PEM format.	No default.
`private-key <prkey>`	The private key in PEM format.	No default.
Fields relevant to SCEP auto-update		
`scep-url <URL_str>`	Enter the URL of the SCEP server.	No default.
`scep-password <password_str>`	Enter the password for the SCEP server.	No default.

Variable	Description	Default
`auto-regenerate-days <days_int>`	Enter how many days before expiry the FortiGate unit requests an updated local certificate. Enter `0` for no auto-update.	`0`
`auto-regenerate-days-warning <days_int>`	Enter how many days before local certificate expiry the FortiGate generates a warning message. Enter 0 for no warning.	`0`

History

FortiOS v3.0 New.

FortiOS v3.0 MR6 Added `comments` field.

FortiOS v4.0 MR1 Added `auto-regenerate-days`, `auto-regenerate-days-warning`, `scep-password`, and `scep-url` fields.

Related topics

- vpn certificate ca
- vpn certificate crl
- vpn certificate ocsp
- vpn certificate remote
- execute vpn certificate local

certificate ocsp

Use this command to install remote certificates. The remote certificates are public certificates without a private key. They are used as OCSP (Online Certificate Status Protocol) server certificates.

Syntax

```
config vpn certificate ocsp
  edit cert <cert_name>
    set url <ocsp_url>
    set unavail-action <unavailable_action>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get vpn certificate ocsp [cert_name]
```

Variable	Description
`cert <cert_name>`	Enter the OCSP server public certificate (one of the remote certificates).
`url <ocsp_url>`	Enter the URL of the OCSP server.
`unavail-action <unavailable_action>`	Action taken on client certification when the OCSP server is unreachable. `revoke` or `ignore`. Default is `revoke`.

History

FortiOS v3.0 MR4 New.

Related topics

- vpn certificate local
- vpn certificate ca
- vpn certificate crl
- vpn certificate remote
- execute vpn certificate remote

certificate remote

Use this command to install remote certificates. The remote certificates are public certificates without a private key. They are used as OCSP (Online Certificate Status Protocol) server certificates.

Syntax

```
config vpn certificate remote
  edit cert <cert_name>
    set remote <remote_cert_detail>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get vpn certificate remote [cert_name]
```

Variable	Description
`cert <cert_name>`	Enter the name of the public certificate.
`remote <remote_cert_detail>`	Details/description of the remote certificate.

History

FortiOS v3.0 MR4 New.

Related topics

- vpn certificate local
- vpn certificate ca
- vpn certificate crl
- vpn certificate ocsp
- execute vpn certificate remote

ipsec concentrator

Use this command to add IPSec policy-based VPN tunnels to a VPN concentrator. The VPN concentrator collects hub-and-spoke tunnels into a group.

The concentrator allows VPN traffic to pass from one tunnel to the other through the FortiGate unit. The FortiGate unit functions as a concentrator, or hub, in a hub-and-spoke network.

Note: VPN concentrators are not available in Transparent mode.

Syntax

```
config vpn ipsec concentrator
  edit <concentrator_name>
    set member <member_name> [member_name] [member_name]
    set src-check {enable | disable}
  end
```

Note: The `member` field is required.

Variable	Description	Default
`edit <concentrator_name>`	Enter a name for the concentrator.	No default.
`member <member_name> [member_name] [member_name]`	Enter the names of up to three VPN tunnels to add to the concentrator. Separate the tunnel names with spaces. Members can be tunnels defined in `vpn ipsec phase1` or `vpn ipsec manual-key`. To add or remove tunnels from the concentrator you must re-enter the whole list with the required additions or deletions.	No default.
`src-check {enable | disable}`	Enable to check the source address of the phase2 selector when locating the best matching phase2 in a concentrator. The default is to check only the destination selector.	disable

Example

Use the following commands to add an IPSec VPN concentrator named `Concen_1` and add three tunnels to the concentrator.

```
config vpn ipsec concentrator
  edit Concen_1
    set member Tunnel_1 Tunnel_2 Tunnel_3
  end
```

History

FortiOS v2.80	Revised.
FortiOS v2.80 MR4	Method for adding concentrators changed.
FortiOS v3.0	Members must now be phase1 configurations, not phase2.
FortiOS v4.0	Added `src-check` field.

Related topics

- vpn ipsec phase1, vpn ipsec manualkey

ipsec forticlient

Use this command to configure automatic VPN configuration for FortiClient Host Security application users.

The FortiClient users who will use automatic configuration must be members of a user group. The `config vpn ipsec forticlient` command creates a “realm” that associates the user group with the phase 2 VPN configuration. You can create multiple realms to associate different user groups with different phase 2 configurations.

The user group identifies the user name and password settings that the dialup client’s credentials must match in order for authentication to be successful. The phase 2 tunnel definition and its associated firewall encryption policy provides the configuration parameters to download to the FortiClient Host Security application.

Syntax

Set or unset VPN policy distribution parameters.

```
config vpn ipsec forticlient
  edit <realm_name>
    set phase2name <tunnel_name>
    set status {disable | enable}
    set usergroupname <group_name>
  end
```

Variable	Description	Default
`edit <realm_name>`	Enter a name for the FortiClient realm. This is also referred to as the policy name.	No default.
`phase2name <tunnel_name>`	Enter the name of the phase 2 tunnel configuration that you defined as part of the dialup-client configuration.	`Null`
`status {disable | enable}`	Enable or disable IPSec VPN policy distribution.	`enable`
`usergroupname <group_name>`	Enter the name of the user group that you created for dialup clients. This group must already exist.	`Null`

Example

The following example enables VPN policy distribution for a user group called `Dialup_users`. The phase 2 tunnel configuration named `FG1toDialup_tunnel` provides the FortiGate unit with the information it needs to find and apply the associated firewall encryption policy:

```
config vpn ipsec forticlient
  edit Standard_VPN_policy
    set phase2name FG1toDialup_tunnel
    set usergroupname Dialup_users
    set status enable
  end
```

History

FortiOS v3.0 New.

Related topics

- vpn ipsec phase2
- user group

ipsec manualkey

Use this command to configure manual keys for IPSec tunnel-mode VPN tunnels. You configure a manual key tunnel to create an IPSec tunnel-mode VPN tunnel between the FortiGate unit and a remote IPSec VPN client or gateway that is also using manual key.

A manual key VPN tunnel consists of a name for the tunnel, the IP address of the VPN gateway or client at the opposite end of the tunnel, and the encryption and authentication algorithms to use for the tunnel. Because the keys are created when you configure the tunnel, no negotiation is required for the VPN tunnel to start. However, the VPN gateway or client that connects to this tunnel must use the same encryption and authentication algorithms and must have the same encryption and authentication keys.

Syntax

```
config vpn ipsec manualkey
  edit <tunnel_name>
    set authentication <authentication_algorithm>
    set authkey <authentication_key>
    set encryption <method>
    set enckey <encryption_key>
    set interface <interface_name>
    set localspi <local_spi_number>
    set local-gw <address_ipv4>
    set remote-gw <address_ipv4>
    set remotespi <remote_spi_number>
  end
```

Note: The `authentication`, `encryption`, `interface`, `remote-gw`, `localspi`, and `remotespi` fields are required. All other fields are optional.

Variable	Description	Default
`edit <tunnel_name>`	Enter a name for the tunnel.	No default.
`authentication <authentication_algorithm>`	Enter one of the following authentication algorithms: • `md5` • `null` • `sha1` • `sha256` Make sure you use the same algorithm at both ends of the tunnel. **Note:** `encryption` and `authentication` cannot both be `null`.	`null`
`authkey <authentication_key>`	This field is available when `authentication` is set to `md5`, `sha1`, or `sha256`. Enter the key in 16-digit (8-byte) segments separated by hyphens. For example (MD5): `0102030405060708-090a0b0c0d0e0f10` For a SHA1 key, the final segment is only 8 digits (4 bytes). • If `authentication` is `md5`, enter a 32-digit (16-byte) hexadecimal number. • If `authentication` is `sha1`, enter a 40-digit (20-byte) hexadecimal number. • If `authentication` is `sha256`, enter a 64-digit (32-byte) hexadecimal number. Digits can be `0` to `9`, and `a` to `f`. Use the same authentication key at both ends of the tunnel.	- (No default.)

Variable	Description	Default
encryption <method>	Enter one of the following encryption algorithms: • 3des • aes128 • aes192 • aes256 • des • null Make sure you use the same algorithm at both ends of the tunnel. **Note:** encryption and authentication cannot both be null.	null
enckey <encryption_key>	This field is available when encryption is set to 3des, aes128, aes192, aes256, or des. Enter the associated encryption key: • If encryption is des, enter a 16 digit (8 byte) hexadecimal number. • If encryption is 3des, enter a 48 digit (24 byte) hexadecimal number. • If encryption is aes128, enter a 32 digit (16 byte) hexadecimal number. • If encryption is aes192, enter a 48 digit (24 byte) hexadecimal number. • If encryption is aes256, enter a 64 digit (32 byte) hexadecimal number. Digits can be 0 to 9, and a to f. For all of the above, separate each 16 digit (8 byte) hexadecimal segment with a hyphen. Use the same encryption key at both ends of the tunnel.	- (No default.)
interface <interface_name>	Enter the name of the physical, aggregate, or VLAN interface to which the IPSec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from system interface settings (see “interface” on page 448). You cannot change interface if a firewall policy references this VPN.	Null.
local-gw <address_ipv4>	Optionally, specify a secondary IP address of the interface selected in interface to use for the local end of the VPN tunnel. If you do not specify an IP address here, the FortiGate unit obtains the IP address of the interface from the system interface settings (see “interface” on page 448).	0.0.0.0
localspi <local_spi_number>	Local Security Parameter Index. Enter a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f) in the range 0x100 to FFFFFFF. This number must be added to the Remote SPI at the opposite end of the tunnel.	0x100
remote-gw <address_ipv4>	The IP address of the remote gateway external interface.	0.0.0.0
remotespi <remote_spi_number>	Remote Security Parameter Index. Enter a hexadecimal number of up to eight digits in the range 0x100 to FFFFFFF. This number must be added to the Local SPI at the opposite end of the tunnel.	0x100

Example

Use the following command to add an IPSec VPN manual key tunnel with the following characteristics:

- Tunnel name: Manual_Tunnel
- Local SPI: 1000ff
- Remote SPI: 2000ff
- Remote gateway IP address: 206.37.33.45
- Encryption algorithm: 3DES
- Encryption keys: 003f2b01a9002f3b 004f4b0209003f01 3b00f23bff003eff

- Authentication algorithm: `MD5`
- Authentication keys: `ff003f012ba900bb 00f402303f0100ff`

```
config vpn ipsec manualkey
  edit Manual_Tunnel
    set localspi 1000ff
    set remotespi 2000ff
    set remote-gw 206.37.33.45
    set encryption 3des
    set enckey 003f2b01a9002f3b-004f4b0209003f01-3b00f23bff003eff
    set authentication md5
    set authkey ff003f012ba900bb-00f402303f0100ff
  end
```

History

FortiOS v2.80	Revised
FortiOS v2.80 MR3	`concentrator` field available in NAT/Route mode only.
FortiOS v3.0	Removed `concentrator` field. Renamed `gateway` field to `remote-gw`. Added `interface` field.
FortiOS v3.0 MR3	Added `local-gw` field.
FortiOS v3.0 MR5	`encryption` and `authentication` cannot both be `null`.

Related topics

- vpn ipsec phase2

ipsec manualkey-interface

Use this command to configure manual keys for a route-based (interface mode) IPSec VPN tunnel. When you create a route-based tunnel, the FortiGate unit creates a virtual IPSec interface automatically. The interface can be modified afterward using the `system network interface` CLI command. This command is available only in NAT/Route mode.

Syntax

```
config vpn ipsec manualkey-interface
  edit <tunnel_name>
    set auth-alg <authentication_algorithm>
    set auth-key <authentication_key>
    set enc-alg <method>
    set enc-key <encryption_key>
    set interface <interface_name>
    set ip-version <4 | 6>
    set local-gw <address_ipv4>
    set local-gw6 <address_ipv6>
    set local-spi <local_spi_number>
    set remote-gw <address_ipv4>
    set remote-gw6 <address_ipv6>
    set remote-spi <remote_spi_number>
  end
```

Note: The `auth-alg`, `enc-alg`, `interface`, `remote-gw`, `local-spi`, and `remote-spi` fields are required. All other fields are optional.

Variable	Description	Default
`edit <tunnel_name>`	Enter a name for the tunnel.	No default.
`auth-alg <authentication_algorithm>`	Enter one of the following authentication algorithms: • `md5` • `null` • `sha1` • `sha256` Make sure you use the same algorithm at both ends of the tunnel. **Note:** `enc-alg` and `auth-alg` cannot both be `null`.	`null`
`auth-key <authentication_key>`	This field is available when `auth-alg` is set to `md5`, sha1 or `sha256`. Enter the key in 16-digit (8-byte) segments separated by hyphens. For example (MD5): `0102030405060708-090a0b0c0d0e0f10` For a SHA1 key, the final segment is only 8 digits (4 bytes). • If `auth-alg` is `md5`, enter a 32-digit (16-byte) hexadecimal number. • If `auth-alg` is `sha1`, enter a 40-digit (20-byte) hexadecimal number. • If `auth-alg` is `sha256`, enter a 64-digit (32-byte) hexadecimal number. Digits can be `0` to `9`, and a to `f`. Use the same authentication key at both ends of the tunnel.	- (No default.)

Variable	Description	Default
enc-alg <method>	Enter one of the following encryption algorithms: • 3des • aes128 • aes192 • aes256 • des • null Make sure you use the same algorithm at both ends of the tunnel. **Note:** enc-alg and auth-alg cannot both be null.	null
enc-key <encryption_key>	This field is available when enc-alg is set to 3des, aes128, aes192, aes256, or des. Enter the associated encryption key: • If enc-alg is des, enter a 16 digit (8 byte) hexadecimal number. • If enc-alg is 3des, enter a 48 digit (24 byte) hexadecimal number. • If enc-alg is aes128, enter a 32 digit (16 byte) hexadecimal number. • If enc-alg is aes192, enter a 48 digit (24 byte) hexadecimal number. • If enc-alg is aes256, enter a 64 digit (32 byte) hexadecimal number. Digits can be 0 to 9, and a to f. For all of the above, separate each 16 digit (8 byte) hexadecimal segment with a hyphen. Use the same encryption key at both ends of the tunnel.	- (No default.)
interface <interface_name>	Enter the name of the physical, aggregate, or VLAN interface to which the IPSec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from system interface settings (see "interface" on page 448).	Null.
ip-version <4 | 6>	Enter 4 for IPv4 encapsulation or 6 for IPv6 encapsulation.	4
local-gw <address_ipv4> local-gw6 <address_ipv6>	By default, the FortiGate unit determines the local gateway IP address from the interface setting. Optionally, you can specify a secondary IP address configured on the same interface. local-gw6 is available when ip-version is 6. local-gw is available when ip-version is 4.	0.0.0.0 for IPv4 :: for IPv6
local-spi <local_spi_number>	Local Security Parameter Index. Enter a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f) in the range 0x100 to FFFFFFF. This number must be added to the Remote SPI at the opposite end of the tunnel.	0x100
remote-gw <address_ipv4> remote-gw6 <address_ipv6>	The IP address of the remote gateway external interface. remote-gw6 is available when ip-version is 6. remote-gw is available when ip-version is 4.	0.0.0.0 for IPv4 :: for IPv6
remote-spi <remote_spi_number>	Remote Security Parameter Index. Enter a hexadecimal number of up to eight digits in the range 0x100 to FFFFFFF. This number must be added to the Local SPI at the opposite end of the tunnel.	0x100

Example

Use the following command to add a route-based (interface-mode) IPSec VPN tunnel having the following characteristics:

- Tunnel name: Manual-inf_tunnel
- Local SPI: 1000ff
- Remote SPI: 2000ff
- VLAN interface name: vlan_1

- Remote gateway IP address: `206.37.33.45`
- Encryption algorithm: `3DES`
- Encryption keys: `003f2b01a9002f3b 004f4b0209003f01 3b00f23bff003eff`
- Authentication algorithm: `MD5`
- Authentication keys: `ff003f012ba900bb 00f402303f0100ff`

```
config vpn ipsec-intf manualkey-interface
  edit Manual-inf_tunnel
    set auth-alg md5
    set auth-key ff003f012ba900bb-00f402303f0100ff
    set enc-alg 3des
    set enc-key 003f2b01a9002f3b-004f4b0209003f01-3b00f23bff003eff
    set interface vlan_1
    set local-spi 1000ff
    set remote-spi 2000ff
    set remote-gw 206.37.33.45
  end
```

History

FortiOS v3.0	New
FortiOS v3.0 MR5	`enc-alg` and `auth-alg` cannot both be `null` Added `ip-version`, `local-gw6` and `remote-gw6` fields.

Related topics

- vpn ipsec phase2-interface

ipsec phase1

Use this command to add or edit IPSec tunnel-mode phase 1 configurations. When you add a tunnel-mode phase 1 configuration, you define how the FortiGate unit and a remote VPN peer (gateway or client) authenticate themselves to each other as part of establishing an IPSec VPN tunnel.

The phase 1 configuration specifies the name of a remote VPN peer, the nature of the connection (static IP, dialup, or dynamic DNS), the encryption and authentication keys for the phase 1 proposal, and the authentication method (preshared key or certificate). For authentication to be successful, the FortiGate unit and the remote VPN peer must be configured with compatible phase 1 settings.

You can change all settings except the `type` setting after you define the configuration: if the address type of a remote peer changes, you must delete the original phase 1 configuration and define a new one. As a general rule, create only one phase 1 configuration per remote VPN peer.

Syntax

```
config vpn ipsec phase1
  edit <gateway_name>
    set add-gw-route {enable | disable}
    set authmethod <authentication_method>
    set authpasswd <password>
    set authusr <user_name>
    set authusrgrp <group_name>
    set dhgrp {1 2 5 14}
    set distance <int>
    set dpd {disable | enable}
    set dpd-retrycount <retry_integer>
    set dpd-retryinterval <seconds> [<milliseconds>]
    set interface <interface_name>
    set keepalive <seconds>
    set keylife <seconds>
    set local-gw <address_ipv4>
    set localid <local_id>
    set mode {aggressive | main}
    set nattraversal {disable | enable}
    set peer <CA_certificate_name>
    set peerid <peer_id>
    set peergrp <certificate_group_name>
    set peertype <authentication_method>
    set priority <prio>
    set proposal <encryption_combination>
    set psksecret <preshared_key>
    set remote-gw <address_ipv4>
    set remotegw-ddns <domain_name>
    set rsa-certificate <server_certificate>
    set type <remote_gw_type>
    set usrgrp <group_name>
    set xauthtype <XAuth_type>
  end
```

Note: A `proposal` value is required. In NAT/Route mode, you must specify `interface`. A `remote-gw` value may be required depending on the value of the `type` attribute. You must also enter a preshared key or a certificate name depending on the value of `authmethod`. All other fields are optional.

Variable	Description	Default
`edit <gateway_name>`	Enter a name (maximum 35 characters) for this gateway. If `type` is `dynamic`, the maximum name length is further reduced depending on the number of dialup tunnels that can be established: by 2 for up to 9 tunnels, by 3 for up to 99 tunnels, 4 for up to 999 tunnels, and so on.	No default.
`add-gw-route {enable | disable}`	Enable to automatically add a route to the remote gateway specified in `remote-gw`. This is effective only when `interface` is an interface that obtains its IP address by DHCP or PPPoE. The route distance is specified in the interface configuration. See "system interface" on page 448.	disable
`authmethod <authentication_method>`	Specify the authentication method: • Enter `psk` to authenticate using a pre-shared key. Use `psksecret` to enter the pre-shared key. • Enter `rsa-signature` to authenticate using a digital certificate. Use `set rsa-certificate` to enter the name of the digital certificate. You must configure certificates before selecting `rsa-signature` here. For more information, see "execute vpn certificate local" on page 754 and "vpn certificate ca" on page 570.	`psk`
`authpasswd <password>`	This field is available when `xauthtype` is set to `client`. Enter the XAuth client password for the FortiGate unit.	No default.
`authusr <user_name>`	This field is available when `xauthtype` is set to `client`. Enter the XAuth client user name for the FortiGate unit.	`Null.`
`authusrgrp <group_name>`	This field is available when `xauthtype` is set to `auto, pap`, or `chap`. When the FortiGate unit is configured as an XAuth server, enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross-referenced. For more information, see "user group" on page 551, "user ldap" on page 555, "user local" on page 558, and "user radius" on page 563.	`Null.`
`dhgrp {1 2 5 14}`	Type `1`, `2`, `5` and/or `14` to select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14 respectively. At least one of the DH group settings on the remote peer or client must be identical to one of the selections on the FortiGate unit.	`5`
`distance <int>`	Configure the administrative distance for routes added when a dialup IPSec connection is established. Using administrative distance you can specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. Distance can be an integer from 1-255. See also router static "distance <distance>" on page 361.	1
`dpd {disable | enable}`	Enable or disable DPD (Dead Peer Detection). DPD detects the status of the connection between VPN peers. Enabling DPD facilitates cleaning up dead connections and establishing new VPN tunnels. DPD is not supported by all vendors and is not used unless DPD is supported and enabled by both VPN peers.	`enable`
`dpd-retrycount <retry_integer>`	This field is available when `dpd` is set to `enable`. The DPD retry count when `dpd` is set to `enable`. Set the number of times that the local VPN peer sends a DPD probe before it considers the link to be dead and tears down the security association (SA). The `dpd-retrycount` range is 0 to 10. To avoid false negatives due to congestion or other transient failures, set the retry count to a sufficiently high value for your network.	3

Variable	Description	Default
`dpd-retryinterval <seconds> [<milliseconds>]`	This field is available when `dpd` is set to `enable`. The DPD (Dead Peer Detection) retry interval is the time that the local VPN peer waits between sending DPD probes. Set the time in seconds plus, optionally, milliseconds. For example, for 2.5 seconds enter 2 500. The range is 1 to 60 seconds, 0 to 999 milliseconds. When the tunnel is starting, or if it has failed, a retry interval of 5 seconds is used if `dpd-retryinterval` is less than 5 seconds.	5
`interface <interface_name>`	Enter the name of the physical, aggregate, or VLAN interface to which the IPSec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from system interface settings (see "interface" on page 448) unless you specify a different IP address using the local-gw <address_ipv4> attribute. You cannot change `interface` if a firewall policy references this VPN.	Null.
`keepalive <seconds>`	This field is available when `nattraversal` is set to `enable`. Set the NAT traversal keepalive frequency. This number specifies (in seconds) how frequently empty UDP packets are sent through the NAT device to make sure that the NAT mapping does not change until P1 and P2 security associations expire. The keepalive frequency can be from 10 to 900 seconds.	10
`keylife <seconds>`	Set the keylife time. The keylife is the amount of time (in seconds) before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service. The range is 120 to 172,800 seconds.	28800
`local-gw <address_ipv4>`	Optionally, specify a secondary IP address of the interface selected in `interface` to use for the local end of the VPN tunnel. If you do not specify an IP address here, the FortiGate unit obtains the IP address of the interface from the system interface settings (see "interface" on page 448).	`0.0.0.0`
`localid <local_id>`	Enter a local ID if the FortiGate unit is functioning as a VPN client and will use the local ID for authentication purposes. If you want to dedicate a tunnel to a FortiGate dialup client, you must assign a unique identifier (local ID) to the FortiGate client. Whenever you configure a unique identifier (local ID) on a FortiGate dialup client, you must enable aggressive mode on the FortiGate dialup server and also specify the identifier as a peer ID on the FortiGate dialup server.	`Null.`
`mode {aggressive | main}`	Enter `aggressive` or `main` (ID Protection) mode. Both modes establish a secure channel. In main mode, identifying information is hidden. Main mode is typically used when both VPN peers have static IP addresses. In aggressive mode, identifying information is exchanged in the clear. When the remote VPN peer or client has a dynamic IP address, or the remote VPN peer or client will be authenticated using an identifier (local ID), you must select Aggressive mode if there is more than one dialup phase 1 configuration for the interface IP address.	`main`
`nattraversal {disable | enable}`	Enable NAT traversal if you expect the IPSec VPN traffic to go through a gateway that performs NAT. If no NAT device is detected, enabling NAT traversal has no effect. Both ends of the VPN must have the same NAT traversal setting. If you enable NAT traversal you can set the `keepalive` frequency.	`enable`

Variable	Description	Default
peer <CA_certificate_name>	This field is available when authmethod is set to rsa-signature and peertype is set to peer. Enter the name of the peer (CA) certificate that will be used to authenticate remote VPN clients or peers. Use the command config user peer to add peer certificates. Peer certificates must be added to the FortiGate configuration before they can be cross-referenced. For more information, see "user peer" on page 560.	Null.
peerid <peer_id>	This field is available when peertype is set to one. Enter the peer ID that will be used to authenticate remote clients or peers by peer ID.	Null.
peergrp <certificate_group_name>	This field is available when type is set to dynamic, authmethod is set to rsa-signature, and peertype is set to peergrp. Enter the name of the peer certificate group that will be used to authenticate remote clients or peers. You must create the peer certificate group before the group name can be cross-referenced. For more information, see "user peergrp" on page 562.	Null.
peertype <authentication_method>	The following attributes are available under the following conditions: • one is available when mode is set to aggressive or when authmethod is set to rsa-signature. • dialup is available when type is set to dynamic and authmethod is set to psk. • peer is available when authmethod is set to rsa-signature. • peergrp is available when type is set to dynamic and authmethod is set to rsa-signature. Enter the method for authenticating remote clients or peers when they connect to the FortiGate unit: • Type any to accept any remote client or peer (peer IDs are not used for authentication purposes). The mode attribute can be set to aggressive or main. You can use this option with RSA Signature authentication. But, for highest security, you should configure a PKI user/group for the peer and set Peer Options to Accept this peer certificate only. • Type one to authenticate either a remote peer or client that has a dynamic IP address and connects using a unique identifier over a dedicated tunnel, or more than one dialup client that connects through the same tunnel using the same (shared) identifier. Use the peerid field to set the peer ID. If more than one dialup client will be connecting using the same (shared) identifier, set mode to aggressive. • Type dialup to authenticate dialup VPN clients that use unique identifiers and preshared keys (or unique preshared keys only) to connect to the VPN through the same VPN tunnel. In this case, you must create a dialup user group for authentication purposes. Use the usrgrp field to set the user group name. If the dialup clients use unique identifiers and preshared keys, set mode to aggressive. If the dialup clients use preshared keys only, set mode to main. • Type peer to authenticate one (or more) certificate holders based on a particular (or shared) certificate. Use the peer field to enter the certificate name. Set mode to aggressive if the remote peer or client has a dynamic IP address. • Type peergrp to authenticate certificate holders that use unique certificates. In this case, you must create a group of certificate holders for authentication purposes. Use the peergrp field to set the certificate group name. The mode attribute can be set to aggressive or main. Set mode to aggressive if the remote peer or client has a dynamic IP address.	any

Variable	Description	Default
priority <prio>	This value is used to be break ties in selection of dialup routes. In the case that both routes have the same priority, the egress index for the routes will be used to determine the selected route. Set <prio> to a value between 0 and 4 294 967 295.	0
proposal <encryption_combination>	Select a minimum of one and a maximum of three encryption-message digest combinations for the phase 1 proposal (for example, 3des-md5). The remote peer must be configured to use at least one of the proposals that you define. Use a space to separate the combinations. You can choose any of the following abbreviated symmetric key encryption algorithms: • des — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3des — Triple-DES, in which plain text is encrypted three times by three keys. • aes128 — A 128-bit block algorithm that uses a 128-bit key. • aes192 — A 128-bit block algorithm that uses a 192-bit key. • aes256 — A 128-bit block algorithm that uses a 256-bit key. You can select any of the following message digests to check the authenticity of messages during an encrypted session: • md5 — Message Digest 5, the hash algorithm developed by RSA Data Security. • sha1 — Secure Hash Algorithm 1, which produces a 160-bit message digest. • sha256 — Secure Hash Algorithm 2, which produces a 256-bit message digest.	aes128-sha1 3des-sha1
psksecret <preshared_key>	This field is available when authmethod is set to psk. Enter the pre-shared key. The pre-shared key must be the same on the remote VPN gateway or client and should only be known by network administrators. The key must consist of at least 6 printable characters. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.	* (No default.)
remote-gw <address_ipv4>	This field is available when type is set to static. Enter the static IP address of the remote VPN peer.	0.0.0.0
remotegw-ddns <domain_name>	This field is available when type is set to ddns. Enter the identifier of the remote peer (for example, a fully qualified domain name). Use this setting when the remote peer has a static domain name and a dynamic IP address (the IP address is obtained dynamically from an ISP and the remote peer subscribes to a dynamic DNS service).	Null.
rsa-certificate <server_certificate>	This field is available when authmethod is set to rsa-signature. Enter the name of the signed personal certificate for the FortiGate unit. You must install the server certificate before you enter the server certificate name. For more information, see "vpn certificate local" on page 754.	Null.
type <remote_gw_type>	Enter the connection type of the remote gateway: • If the remote VPN peer has a static IP address, type static. Use the remotegw field to enter the IP address. • If the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE), type dynamic. • If the remote VPN peer has a dynamically assigned IP address and subscribes to a dynamic DNS service, type ddns. Use the remotegw-ddns field to enter the domain name of the remote VPN peer.	static

Variable	Description	Default
usrgrp <group_name>	This field is available when type is set to dynamic, authmethod is set to psk, and peertype is set to dialup. Enter the name of the group of dialup VPN clients to authenticate. The user group must be added to the FortiGate configuration before it can be cross-referenced here. For more information, see "user group" on page 551, "user ldap" on page 555, "user local" on page 558, and "user radius" on page 563.	Null.
xauthtype <XAuth_type>	Optionally configure XAuth (eXtended Authentication): • Type disable to disable XAuth. • Type client to configure the FortiGate unit to act as an XAuth client. Use the authuser field to add the XAuth user name and password. • Type auto, pap, or chap to configure the FortiGate unit as an XAuth server. These options are available only when type is dynamic. Use the authusrgrp field to specify the user group containing members that will be authenticated using XAuth.	disable

Example

Use the following command to add a tunnel-mode IPSec VPN phase 1 configuration with the following characteristics:

- Phase 1 configuration name: Simple_GW
- Physical interface name: port6
- Remote peer address type: Dynamic
- Encryption and authentication proposal: des-md5
- Authentication method: psk
- Pre-shared key: Qf2p3O93jIj2bz7E
- Mode: aggressive
- Dead Peer Detection: disable

```
config vpn ipsec phase1
  edit Simple_GW
    set interface port6
    set type dynamic
    set proposal des-md5
    set authmethod psk
    set psksecret Qf2p3O93jIj2bz7E
    set mode aggressive
    set dpd disable
  end
```

History

FortiOS v2.80	Revised
FortiOS v2.80 MR2	Added two new options to the peertype field: peer and peergrp. Added two new fields: peer and peergrp.

FortiOS v3.0	Renamed `mixed` option of `xauthtype` field to `auto`. Renamed `remotegw` to `remote-gw`. Added `interface` and `local-gw` attributes. Name of phase 1 definition is now limited to 15 characters. Added `priority` field.
FortiOS v4.0	Changed default value of `proposal` to `aes128-sha1 3des-sha1`. Changed default value of `dpd` and `nattraversal` to `enable`.

Related topics

- vpn ipsec phase2
- user group
- user local
- user peer
- user peergrp
- user radius
- execute vpn certificate local
- vpn certificate ca

ipsec phase1-interface

Use this command to define a phase 1 definition for a route-based (interface mode) IPSec VPN tunnel that generates authentication and encryption keys automatically. A new interface of type “tunnel” with the same name is created automatically as the local end of the tunnel.

Optionally, you can create a route-based phase 1 definition to act as a backup for another IPSec interface. See the monitor-phase1 <phase1> field.

To complete the configuration of an IPSec tunnel, you need to:

- configure phase 2 settings (see “ipsec phase2-interface” on page 611)
- configure a firewall policy to pass traffic from the local private network to the tunnel interface
- configure a static route via the IPSec interface to the private network at the remote end of the tunnel
- optionally, define the IP addresses for each end of the tunnel to enable dynamic routing through the tunnel or to enable pinging of each end of the tunnel for testing

Syntax

```
config vpn ipsec phase1-interface
  edit <gateway_name>
    set add-gw-route {enable | disable}
    set add-route {enable | disable}
    set assign-ip {enable | disable}
    set assign-ip-from {range | usrgrp}
    set assign-ip-type {ip | subnet}
    set authmethod <authentication_method>
    set authpasswd <password>
    set authusr <user_name>
    set authusrgrp <group_name>
    set banner <string>
    set default-gw <gw_ip>
    set default-gw-priority <int>
    set dhgrp {1 2 5 14}
    set distance <int>
    set domain <string>
    set dpd {disable | enable}
    set dpd-retrycount <retry_integer>
    set dpd-retryinterval <seconds> [<milliseconds]
    set ike-version {1 | 2}
    set interface <interface_name>
    set ip-version <4 | 6>
    set ipv4-dns-server1
    set ipv6-dns-server1
    set ipv4-dns-server2
    set ipv6-dns-server2
    set ipv4-dns-server3
    set ipv6-dns-server3
    set ipv4-end-ip <ip4addr>
    set ipv6-end-ip <ip6addr>
    set ipv4-netmask <ip4mask>
    set ipv4-split-include <address_name>
    set ipv4-start-ip <ip4addr>
    set ipv6-start-ip <ip6addr>
    set ipv4-wins-server1
```

```
    set ipv4-wins-server2
    set ipv6-prefix <ip6prefix>
    set keepalive <seconds>
    set keylife <seconds>
    set local-gw <address_ipv4>
    set local-gw6 <address_ipv6>
    set localid <local_id>
    set mode {aggressive | main}
    set mode-cfg {enable | disable}
    set mode-cfg-ip-version {4|6}
    set monitor-phase1 <phase1>
    set nattraversal {disable | enable}
    set peer <CA_certificate_name>
    set peerid <peer_id>
    set peergrp <certificate_group_name>
    set peertype <authentication_method>
    set priority <prio>
    set proposal <encryption_combination>
    set psksecret <preshared_key>
    set remote-gw <address_ipv4>
    set remote-gw6 <address_ipv6>
    set remotegw-ddns <domain_name>
    set rsa-certificate <server_certificate>
    set type <remote_gw_type>
    set unity-support {enable | disable}
    set usrgrp <group_name>
    set xauthtype <XAuth_type>
    config ipv4-exclude-range
      edit <entry_id>
        set start-ip <ipaddr>
        set end-ip <ipaddr>
      end
    config ipv6-exclude-range
      edit <entry_id>
        set start-ip <ipaddr>
        set end-ip <ipaddr>
      end
  end
```

Note: You must specify values for `proposal` and `interface`. A `remote-gw` value may be required depending on the value of the `type` attribute. You must also enter a preshared key or a certificate name depending on the value of `authmethod`. All other fields are optional.

Variable	Description	Default
`edit <gateway_name>`	Enter a name (maximum 15 characters) for the remote gateway. If `type` is `dynamic`, the maximum name length is further reduced depending on the number of dialup tunnels that can be established: by 2 for up to 9 tunnels, by 3 for up to 99 tunnels, 4 for up to 999 tunnels, and so on	No default.
`add-gw-route {enable | disable}`	Enable to automatically add a route to the remote gateway specified in `remote-gw`. This is effective only when `interface` is an interface that obtains its IP address by DHCP or PPPoE. The route distance is specified in the interface configuration. See “system interface” on page 448.	disable

Variable	Description	Default
add-route {enable | disable}	Enable to add a route to the client's peer destination selector. Disable if you use dynamic routing over the tunnel. This is available only when mode-cfg is enabled.	enable
assign-ip {enable | disable}	For a client, enable to request an IP address from the server. For a server, enable to assign an IP address to a dialup client. This is available if mode-cfg (IKE Configuration Method) is enabled.	enable
assign-ip-from {range | usrgrp}	Select source of IP address assigned to an IKE Configuration Method client. range — Assign an IP address from the range defined in ipv4-start-ip and ipv4-end-ip (ipv6-start-ip and ipv4-end-ip for IPv6 clients). usrgrp — Assign the address defined in the RADIUS Framed-IP-Address for the user. This is available when the VPN is configured to authenticate clients with XAuth. xauthtype must be auto, pap, or chap. This is available if mode-cfg (IKE Configuration Method) is enabled.	range
assign-ip-type {ip | subnet}	Select the type of IP address assigned to an IKE Configuration Method client: ip — assign a single IP address to the client, as configured in assign-ip-from. subnet — assign an IP address to each end of the VPN tunnel, as configured in assign-ip-from. This type of IP address assignment facilitates the use of dynamic routing through the tunnel. This is available if mode-cfg (IKE Configuration Method) is enabled.	ip
authmethod <authentication_method>	Specify the authentication method: • Enter psk to authenticate using a pre-shared key. Use psksecret to enter the pre-shared key. • Enter rsa-signature to authenticate using a digital certificate. Use set rsa-certificate to enter the name of the digital certificate. You must configure certificates before selecting rsa-signature here. For more information, see "execute vpn certificate local" on page 754 and "vpn certificate ca" on page 570.	psk
authpasswd <password>	This field is available when xauthtype is set to client. Enter the XAuth client password for the FortiGate unit.	No default.
authusr <user_name>	This field is available when xauthtype is set to client. Enter the XAuth client user name for the FortiGate unit.	Null
authusrgrp <group_name>	This field is available when xauthtype is set to auto, pap, or chap. When the FortiGate unit is configured as an XAuth server, enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross-referenced. For more information, see "user group" on page 551, "user ldap" on page 555, "user local" on page 558, and "user radius" on page 563.	Null
banner <string>	Specify a message to send to IKE Configuration Method clients. Some clients display this message to users. This is available if mode-cfg (IKE Configuration Method) is enabled.	Null

Variable	Description	Default
default-gw <gw_ip>	If the IPSec interface has a different default route than other traffic, enter the next hop router IP address. Be sure to set default-gw-priority to a higher priority (lower value) than the general default route. This is available when type is dynamic. The route it creates is not visible in the routing table.	0.0.0.0
default-gw-priority <int>	If you set default-gw, set the priority to a lower value (higher priority) than the general default route.	0
dhgrp {1 2 5 14}	Type 1, 2, 5, and/or 14 to select one or more Diffie-Hellman groups from DH group 1, 2, 5, and 14 respectively. At least one of the DH group settings on the remote peer or client must be identical to one of the selections on the FortiGate unit.	5
distance <int>	Configure the administrative distance for routes added when a dialup IPSec connection is established. Using administrative distance you can specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. Distance can be an integer from 1-255. See also router static "distance <distance>" on page 361.	1
domain <string>	Specify a domain name to send to IKE Configuration Method clients. This is available if mode-cfg (IKE Configuration Method) is enabled.	Null
dpd {disable | enable}	Enable or disable DPD (Dead Peer Detection). DPD detects the status of the connection between VPN peers. Enabling DPD facilitates cleaning up dead connections and establishing new VPN tunnels. DPD is not supported by all vendors and is not used unless DPD is supported and enabled by both VPN peers.	enable
dpd-retrycount <retry_integer>	This field is available when dpd is set to enable. The DPD retry count when dpd is set to enable. Set the number of times that the local VPN peer sends a DPD probe before it considers the link to be dead and tears down the security association (SA). The dpd-retrycount range is 0 to 10. To avoid false negatives due to congestion or other transient failures, set the retry count to a sufficiently high value for your network.	3
dpd-retryinterval <seconds> [<milliseconds]	This field is available when dpd is set to enable. The DPD (Dead Peer Detection) retry interval is the time that the local VPN peer waits between sending DPD probes. Set the time in seconds plus, optionally, milliseconds. For example, for 2.5 seconds enter 2 500. The range is 1 to 60 seconds, 0 to 999 milliseconds. When the tunnel is starting, or if it has failed, a retry interval of 5 seconds is used if dpd-retryinterval is less than 5 seconds.	5
ike-version {1 | 2}	Select whether to use IKEv1 or IKEv2 (RFC 4306).	1
interface <interface_name>	Enter the name of the physical, aggregate, or VLAN interface to which the IPSec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from system interface settings (see "interface" on page 448) unless you specify a different IP address using the local-gw <address_ipv4> attribute.	Null.
ip-version <4 | 6>	Enter 4 for IPv4 encapsulation or 6 for IPv6 encapsulation.	4
ipv4-dns-server1 ipv6-dns-server1 ipv4-dns-server2 ipv6-dns-server2 ipv4-dns-server3 ipv6-dns-server3	Enter DNS server addresses to provide to IKE Configuration Method clients. If the value is 0.0.0.0, no DNS server address is provided. Either the IPv4 or IPv6 version of these fields is available, depending on mode-cfg-ip-version.	0.0.0.0 ::

Variable	Description	Default
ipv4-end-ip <ip4addr> ipv6-end-ip <ip6addr>	Set end of IP address range to assign to IKE Configuration Method clients. This is available when mode-cfg is enabled, type is dynamic, and assign-ip-from is range. Either the IPv4 or IPv6 version of this field is available, depending on mode-cfg-ip-version.	No default.
ipv4-netmask <ip4mask>	Set the netmask value to pass to IKE Configuration Method clients.	No default.
ipv4-split-include <address_name>	Select the address or address group that the client can reach through the VPN. This information is sent to the client as part of IKE Configuration Method.	Null.
ipv4-start-ip <ip4addr> ipv6-start-ip <ip6addr>	Set start of IP address range to assign to IKE Configuration Method clients. This is available when mode-cfg is enabled, type is dynamic, and assign-ip-from is range. Either the IPv4 or IPv6 version of this field is available, depending on mode-cfg-ip-version.	No default.
ipv4-wins-server1 ipv4-wins-server2	Enter WINS server addresses to provide to IKE Configuration Method clients. If the value is 0.0.0.0, no WINS server address is provided.	0.0.0.0
ipv6-prefix <ip6prefix>	Specify the size, in bits, of the network portion of the subnet address for IPv6 IKE Configuration Method clients. Range is 0 to 128. This is available when mode-cfg-ip-version is 6 and assign-ip-type is subnet.	0
keepalive <seconds>	This field is available when nattraversal is set to enable. Set the NAT traversal keepalive frequency. This number specifies (in seconds) how frequently empty UDP packets are sent through the NAT device to make sure that the NAT mapping does not change until P1 and P2 security associations expire. The keepalive frequency can be from 0 to 900 seconds.	5
keylife <seconds>	Set the keylife time. The keylife is the amount of time (in seconds) before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service. The range is 120 to 172,800 seconds.	28800
local-gw <address_ipv4> local-gw6 <address_ipv6>	Optionally, specify a secondary IP address of the interface selected in interface to use for the local end of the VPN tunnel. local-gw6 is available when ip-version is 6. local-gw is available when ip-version is 4. If you do not specify an IP address here, the FortiGate unit obtains the IP address of the interface from system interface settings (see "interface" on page 448).	0.0.0.0 for IPv4 :: for IPv6
localid <local_id>	Enter a local ID if the FortiGate unit is functioning as a VPN client and will use the local ID for authentication purposes. If you want to dedicate a tunnel to a FortiGate dialup client, you must assign a unique identifier (local ID) to the FortiGate client. Whenever you configure a unique identifier (local ID) on a FortiGate dialup client, you must enable aggressive mode on the FortiGate dialup server and also specify the identifier as a peer ID on the FortiGate dialup server.	Null.
mode {aggressive | main}	Enter aggressive or main (ID Protection) mode. Both modes establish a secure channel. In main mode, identifying information is hidden. Main mode is typically used when both VPN peers have static IP addresses. In aggressive mode, identifying information is exchanged in the clear. Aggressive mode is typically used when a remote peer or dialup client has a dynamic IP address. You must enable aggressive mode when the remote FortiGate unit has a dynamic IP address, or the remote VPN peer or client will be authenticated using an identifier (local ID). This is available if ike-version is 1.	main

Variable	Description	Default
mode-cfg {enable | disable}	Enable IKE Configuration Method so that compatible clients can configure themselves with settings that the FortiGate unit provides. This is available if type is dynamic and ike-version is 1.	disable
mode-cfg-ip-version {4|6}	Select whether an IKE Configuration Method client receives an IPv4 or IPv6 IP address. This is available if mode-cfg and assign-ip are enabled.	4
monitor-phase1 <phase1>	Optionally, this IPSec interface can act as a backup for another (primary) IPSec interface. Enter the name of the primary interface. The backup interface is used only while the primary interface is out of service. dpd must be enabled. A primary interface can have only one backup interface and cannot act as a backup for another interface. For a configuration example, see “Example of backup IPSec interface” on page 602.	Null.
nattraversal {disable | enable}	Enable NAT traversal if you expect the IPSec VPN traffic to go through a gateway that performs NAT. If no NAT device is detected, enabling NAT traversal has no effect. Both ends of the VPN must have the same NAT traversal setting. If you enable NAT traversal you can set the keepalive frequency.	enable
peer <CA_certificate_name>	This field is available when authmethod is set to rsa-signature and peertype is set to peer. Enter the name of the peer (CA) certificate that will be used to authenticate remote VPN clients or peers. Use the command config user peer to add peer certificates. Peer certificates must be added to the FortiGate configuration before they can be cross-referenced. For more information, see “user peer” on page 560.	Null.
peerid <peer_id>	This field is available when peertype is set to one. Enter the peer ID that will be used to authenticate remote clients or peers by peer ID.	Null.
peergrp <certificate_group_name>	This field is available when type is set to dynamic, authmethod is set to rsa-signature, and peertype is set to peergrp. Enter the name of the peer certificate group that will be used to authenticate remote clients or peers. You must create the peer certificate group before the group name can be cross-referenced. For more information, see “user peergrp” on page 562.	Null.

Variable	Description	Default
peertype <authentication_method>	The following attributes are available under the following conditions: • dialup is available when type is set to dynamic and authmethod is set to psk. • peer is available when authmethod is set to rsa-signature. • peergrp is available when type is set to dynamic and authmethod is set to rsa-signature. Enter the method for authenticating remote clients or peers when they connect to the FortiGate unit: • Type any to accept any remote client or peer (peer IDs are not used for authentication purposes). The mode attribute can be set to aggressive or main. You can use this option with RSA Signature authentication. But, for highest security, you should configure a PKI user/group for the peer and set Peer Options to Accept this peer certificate only. • Type one to authenticate either a remote peer or client that has a dynamic IP address and connects using a unique identifier over a dedicated tunnel, or more than one dialup client that connects through the same tunnel using the same (shared) identifier. Use the peerid field to set the peer ID. If more than one dialup client will be connecting using the same (shared) identifier, set mode to aggressive. • Type dialup to authenticate dialup VPN clients that use unique identifiers and preshared keys (or unique preshared keys only) to connect to the VPN through the same VPN tunnel. In this case, you must create a dialup user group for authentication purposes. Use the usrgrp field to set the user group name. If the dialup clients use unique identifiers and preshared keys, set mode to aggressive. If the dialup clients use preshared keys only, set mode to main. • Type peer to authenticate one (or more) certificate holders based on a particular (or shared) certificate. Use the peer field to enter the certificate name. Set mode to aggressive if the remote peer or client has a dynamic IP address. • Type peergrp to authenticate certificate holders that use unique certificates. In this case, you must create a group of certificate holders for authentication purposes. Use the peergrp field to set the certificate group name. The mode attribute can be set to aggressive or main. Set mode to aggressive if the remote peer or client has a dynamic IP address.	any
priority <prio>	This value is used to be break ties in selection of dialup routes. In the case that both routes have the same priority, the egress index for the routes will be used to determine the selected route. Set <prio> to a value between 0 and 4 294 967 295.	0

Variable	Description	Default
proposal <encryption_combination>	Select a minimum of one and a maximum of three encryption-message digest combinations for the phase 1 proposal (for example, 3des-md5). The remote peer must be configured to use at least one of the proposals that you define. Use a space to separate the combinations. You can choose any of the following abbreviated symmetric key encryption algorithms: • des — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3des — Triple-DES, in which plain text is encrypted three times by three keys. • aes128 — A 128-bit block algorithm that uses a 128-bit key. • aes192 — A 128-bit block algorithm that uses a 192-bit key. • aes256 — A 128-bit block algorithm that uses a 256-bit key. You can select any of the following message digests to check the authenticity of messages during an encrypted session: • md5 — Message Digest 5, the hash algorithm developed by RSA Data Security. • sha1— Secure Hash Algorithm 1, which produces a 160-bit message digest. • sha256 — Secure Hash Algorithm 2, which produces a 256-bit message digest.	aes128-sha1 3des-sha1
psksecret <preshared_key>	This field is available when authmethod is set to psk. Enter the pre-shared key. The pre-shared key must be the same on the remote VPN gateway or client and should only be known by network administrators. The key must consist of at least 6 printable characters. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.	* (No default.)
remote-gw <address_ipv4> remote-gw6 <address_ipv6>	This field is available when type is set to static. Enter the static IP address of the remote VPN peer. remote-gw6 is available when ip-version is 6. remote-gw is available when ip-version is 4.	0.0.0.0 for IPv4 :: for IPv6
remotegw-ddns <domain_name>	This field is available when type is set to ddns and ip-version is set to 4. Enter the identifier of the remote peer (for example, a fully qualified domain name). Use this setting when the remote peer has a static domain name and a dynamic IP address (the IP address is obtained dynamically from an ISP and the remote peer subscribes to a dynamic DNS service).	Null
rsa-certificate <server_certificate>	This field is available when authmethod is set to rsa-signature. Enter the name of the signed personal certificate for the FortiGate unit. You must install the server certificate before you enter the server certificate name. For more information, see "vpn certificate local" on page 754.	Null
type <remote_gw_type>	Enter the connection type of the remote gateway: • If the remote VPN peer has a static IP address, type static. Use the remotegw field to enter the IP address. • If the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE), type dynamic. • If the remote VPN peer has a dynamically assigned IP address and subscribes to a dynamic DNS service, type ddns. Use the remotegw-ddns field to enter the domain name of the remote VPN peer. This option is not available if ip-version is 6.	static
unity-support {enable | disable}	Enable support for Cisco Unity IKE Configuration Method extensions in either a server or a client.	enable

Variable	Description	Default
usrgrp <group_name>	This field is available when type is set to dynamic, authmethod is set to psk, and peertype is set to dialup. Enter the name of the group of dialup VPN clients to authenticate. The user group must be added to the FortiGate configuration before it can be cross-referenced here. For more information, see "user group" on page 551, "user ldap" on page 555, "user local" on page 558, and "user radius" on page 563.	Null.
xauthtype <XAuth_type>	Optionally configure XAuth (eXtended Authentication): • Type disable to disable XAuth. • Type client to configure the FortiGate unit to act as an XAuth client. Use the authuser field to add the XAuth user name and password. • Type auto, pap, or chap to configure the FortiGate unit as an XAuth server. These options are available only when type is dynamic. Use the authusrgrp field to specify the user group containing members that will be authenticated using XAuth.	disable
config ipv4-exclude-range and config ipv6-exclude-range **Variables** This subcommand is available only when mode-cfg is enabled.		
start-ip <ipaddr>	Enter the start of the exclude range.	No default.
end-ip <ipaddr>	Enter the end of the exclude range.	No default.

Example of route-based VPN

In this example, an IPSec tunnel is needed between two sites using FortiGate units. Users on the 192.168.2.0/24 network at Site A need to communicate with users on the 192.168.3.0/24 network at Site B. At Site A, the public IP address is 172.16.67.199 and at Site B it is 172.16.68.198. At both ends:

- Port 2 of the FortiGate unit: connects to the private network
- Port 1 of the FortiGate unit: connects to the Internet
- Encryption and authentication proposal: des-md5
- Authentication method: psk
- Pre-shared key: Qf2p3O93jIj2bz7
- Mode: main
- Dead Peer Detection: enable

Site A configuration

```
config vpn ipsec phase1-interface
  edit toSiteB
    set type static
    set remote-gw 172.16.68.198
    set interface port1
    set proposal des-md5
    set authmethod psk
    set psksecret Qf2p3O93jIj2bz7
    set mode main
    set dpd enable
  end
```

Site B configuration

```
config vpn ipsec phase1-interface
  edit toSiteA
    set type static
    set remote-gw 172.16.68.199
    set interface port1
    set proposal des-md5
    set authmethod psk
    set psksecret Qf2p3O93jIj2bz7
    set mode main
    set dpd enable
    end
```

```
config vpn ipsec phase2-interface
  edit New_Tunnel
    set phase1name toSiteB
    set proposal 3des-sha1
    set keylife-type seconds
    set keylifeseconds 18001
    set dhgrp 2
    set replay enable
    set pfs enable
    set keepalive enable
  end
config firewall policy
  edit 1
    set srcintf port2
    set dstintf toSiteB
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toSiteB
    set dstintf port2
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  end

config route static
  edit 1
    set device toSiteB
    set dst 192.168.3.0/24
  end
```

```
config vpn ipsec phase2-interface
  edit New_Tunnel
    set phase1name toSiteA
    set proposal 3des-sha1
    set keylife-type seconds
    set keylifeseconds 18001
    set dhgrp 2
    set replay enable
    set pfs enable
    set keepalive enable
  end
config firewall policy
  edit 1
    set srcintf port2
    set dstintf toSiteA
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  next
  edit 2
    set srcintf toSiteA
    set dstintf port2
    set srcaddr all
    set dstaddr all
    set action accept
    set service ANY
    set schedule always
  end

config route static
  edit 1
    set device toSiteA
    set dst 192.168.2.0/24
  end
```

In this example, the user defines IP addresses for each end of the tunnel to enable dynamic routing through the tunnel or to enable pinging of each end of the tunnel for testing. The Site A end has the IP address 10.0.0.1 and the SiteB end is 10.0.0.2.

Site A configuration
(Optional)

```
config system interface
  edit toSiteB
    set ip 10.0.0.1/32
    set remote-ip 10.0.0.2
    set allowaccess ping
  end
```

Site B configuration
(Optional)

```
config system interface
  edit toSiteA
    set ip 10.0.0.2/32
    set remote-ip 10.0.0.1
    set allowaccess ping
  end
```

Example of backup IPSec interface

In this example, the backupToHeadquarters IPSec interface provides failover protection for the toHeadquarters IPSec interface.

The backupToHeadquarters interface is a backup interface because its `monitor-phase1` option is not null; it is set to monitor the toHeadquarters interface. If the monitored interface goes down, as determined by Dead Peer Detection, the backup interface becomes active.

The backup interface uses a different physical interface, which could be connected to a different Internet service provider. The remote gateway can be the same, or it can specify an alternative gateway, if one exists. Otherwise, the two IPSec interfaces are identically configured.

```
config vpn ipsec phase1-interface
  edit "toHeadquarters"
    set interface "wan1"
    set remote-gw 172.16.1.10
    set dpd enable
    ... [other phase1 settings as needed]
  next
  edit "backupToHeadquarters"
    set interface "wan2"
    set monitor-phase1 "toHeadquarters"
    set remote-gw 172.16.1.10
    ... [other phase1 settings as needed]
  end
end
```

IKE Configuration Method

FortiOS supports automatic configuration of IPsec VPNs using the proposed IKE Configuration Method described in *draft-dukes-ike-mode-cfg-02*. Several network equipment vendors support IKE Configuration Method, which is an alternative to DHCP over IPSec.

Dialup VPN clients connect to a FortiGate unit that acts as a VPN server, providing the client the necessary configuration information to establish a VPN tunnel. The configuration information typically includes a virtual IP address, netmask, and DNS server address.

IKE Configuration Method is available only for VPNs that are interface-based, also known as route-based. A FortiGate unit can function as either an IKE Configuration Method server or client.

The `mode-cfg` field enables IKE Configuration Method. The `type` field, although unchanged from previous releases, determines whether you are creating a server or a client. Setting `type` to `dynamic` creates a server configuration, otherwise the configuration is a client.

Required fields to configure a server are `interface`, `proposal`, either `ip4-start-ip`, `ip4-end-ip` and `ipv4-netmask` or `ip6-start-ip`, `ip6-end-ip` and `ip6-prefix`, depending on the value of `mode-cfg-ip-version`. Required fields to configure a client are `interface`, `remote-gw`, and `proposal`.

History

FortiOS v3.0	New
FortiOS v3.0 MR5	Added fields `ip-version`, `local-gw6`, `remote-gw6`.
FortiOS v3.0 MR6	Added fields `default-gw` and `default-gw-priority`.
FortiOS v4.0	Changed default value of `proposal` to `aes128-sha1 3des-sha1`. Changed default value of `dpd` and `nattraversal` to `enable`.
FortiOS v4.0 MR1	Added `ike-version`. Added `sha256` option for `proposal`. Added `14` option to `dhgrp`. Added `mode-cfg` and related fields `add-route`, `assign-ip`, `assign-ip-from`, `assign-ip-type`, `banner`, `domain`, `end-ip`, `mode-cfg-ip-version`, `ipv4-dns-server1`, `ipv6-dns-server1`, `ipv4-dns-server2`, `ipv6-dns-server2`, `ipv4-dns-server3`, `ipv6-dns-server3`, `ipv4-end-ip`, `ipv6-end-ip`, `ipv4-netmask`, `ipv4-split-include`, `ipv4-start-ip`, `ipv6-start-ip`, `ipv4-wins-server1`, `ipv4-wins-server2`, `ipv6-prefix`, `start-ip`, `unity-support`.

Related topics

- vpn ipsec phase2-interface
- user group
- user local
- user peer
- user peergrp
- user radius
- vpn certificate local
- vpn certificate ca

ipsec phase2

Use this command to add or edit an IPSec tunnel-mode phase 2 configuration. The FortiGate unit uses the tunnel-mode phase 2 configuration to create and maintain an IPSec VPN tunnel with a remote VPN peer (the VPN gateway or client).

The phase 2 configuration consists of a name for the VPN tunnel, the name of an existing phase 1 configuration, the proposal settings (encryption and authentication algorithms) and DH group used for phase 2. For phase 2 to be successful, the FortiGate unit and the remote VPN peer must be configured with compatible proposal settings.

Syntax

```
config vpn ipsec phase2
  edit <tunnel_name>
    set add-route {enable | disable}
    set auto-negotiate {enable | disable}
    set dhcp-ipsec {disable | enable}
    set dhgrp {1 | 2 | 5 | 14}
    set dst-addr-type <type>
    set dst-end-ip <address_ipv4>
    set dst-name <address_name>
    set dst-port <destination_port_number>
    set dst-start-ip <address_ipv4>
    set dst-subnet <address_ipv4mask>
    set keepalive {disable | enable}
    set keylife-type <keylife_type>
    set keylifekbs <kb_integer>
    set keylifeseconds <seconds>
    set pfs {disable | enable}
    set phase1name <gateway_name>
    set proposal <encryption_combination>
    set protocol <protocol_integer>
    set replay {disable | enable}
    set route-overlap {overlap_option}
    set selector-match <match_type>
    set single-source {disable | enable}
    set src-addr-type <ip_source_name>
    set src-end-ip <address_ipv4>
    set src-name <address_name>
    set src-port <source_port_number>
    set src-start-ip <address_ipv4>
    set src-subnet <address_ipv4mask>
    set use-natip {enable | disable}
  end
```

Note: The `phase1name` field is required. All other fields are optional.

Variable	Description	Default
`edit <tunnel_name>`	Enter a name for the tunnel.	No default.
`add-route {enable | disable}`	Enable only if you are running a dynamic routing protocol (RIP, OSPF, or BGP) and want the routes to be propagated to routing peers.	disable
`auto-negotiate {enable | disable}`	Enable to negotiate the phase 2 security association (SA) automatically, even if there is no traffic. This repeats every five seconds until it succeeds. You can use this option on a dialup peer to ensure that the tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the tunnel does not exist until the dialup peer initiates traffic.	disable
`dhcp-ipsec {disable | enable}`	This field is available when `phase1name` names a dialup gateway configuration. Enable `dhcp-ipsec` if the FortiGate unit acts as a dialup server and FortiGate DHCP relay will be used to assign VIP addresses to FortiClient dialup clients. The DHCP relay parameters must be configured separately. If you configure the DHCP server to assign IP addresses based on RADIUS user group attributes, you must also set the `peertype` to `dialup` and specify the `usrgrp` in vpn ipsec phase1. For information about how to configure a DHCP server on a FortiGate interface, see "system dhcp server" on page 410. For information about FortiGate DHCP relay, see "system interface" on page 448. If the FortiGate unit acts as a dialup server and you manually assigned FortiClient dialup clients VIP addresses that match the network behind the dialup server, select Enable to cause the FortiGate unit to act as a proxy for the dialup clients.	`disable`
`dhgrp {1 | 2 | 5 | 14}`	Type `1`, `2`, `5`, or `14` to select the Diffie-Hellman group to propose for Phase 2 of the IPSec VPN connection. Both VPN peers must use the same DH Group.	`5`
`dst-addr-type <type>`	Enter the type of destination address that corresponds to the recipient(s) or network behind the remote VPN peer or FortiGate dialup client: • To specify the IP address of a server or host, type `ip`. Enter the IP address using the `dst-start-ip` field. • To specify a range of IP addresses, type `range`. Enter the starting and ending addresses using the `dst-start-ip`, and `dst-end-ip` fields. • To specify a network address, type `subnet`. Enter the network address using the `dst-subnet` field. • To specify a firewall address or address group, type `name`. Enter the address or address group name using the `dst-name` field. You must also select the `name` option for `src-addr-type`. This option is intended for users upgrading VPN configurations created using FortiOS 2.80. For new VPNs that use firewall addresses or address groups as selectors, interface mode VPNs are recommended.	`subnet`
`dst-end-ip <address_ipv4>`	This field is available when `dst-addr-type` is set to `range`. This field is not available if `phase1name` names a configuration that enables `mode-cfg`. Enter the highest destination IP address in the range of IP addresses.	`0.0.0.0`
`dst-name <address_name>`	This field is available when `dst-addr-type` is set to `name`. Enter the name of a firewall address or address group.	No default.

Variable	Description	Default
dst-port <destination_port_number>	Enter the port number that the remote VPN peer or FortiGate dialup client uses to transport traffic related to the specified service (see protocol). The range is 1 to 65535. To specify all ports, type 0.	0
dst-start-ip <address_ipv4>	This field is available when dst-addr-type is set to range. Enter the lowest destination IP address in the range of IP addresses.	0.0.0.0
dst-subnet <address_ipv4mask>	Enter the IP address and network mask that identifies the private network behind the remote VPN peer or FortiGate dialup client.	0.0.0.0 0.0.0.0
keepalive {disable | enable}	Enable to automatically negotiate a new phase 2 security association (SA) before the current SA expires, keeping the tunnel up. Otherwise, a new SA is negotiated only if there is traffic.	disable
keylife-type <keylife_type>	Set when the phase 2 key expires. When the key expires, a new key is generated without interrupting service. • To make the key expire after a period of time has expired and after an amount of data is transmitted, type both. • To make the key expire after an amount of data is transmitted, type kbs. Use the keylifekbs field to set the amount of data that is transmitted. • To make the key expire after a number of seconds elapses, type seconds. Use the keylifeseconds field to set the amount of time that elapses.	seconds
keylifekbs <kb_integer>	This field is available when keylife-type is set to kbs or both. Set the number of KBytes of data to transmit before the phase 2 key expires. The range is 5120 to 99999 KBytes.	5120
keylifeseconds <seconds>	This field is available when keylife-type is set to seconds or both. Set the number of seconds to elapse before the phase 2 key expires. seconds can be 120 to 172800 seconds.	1800
pfs {disable | enable}	Optionally, enable or disable perfect forward secrecy (PFS). PFS ensures that each key created during Phase 2 is unrelated to keys created during Phase 1 or to other keys created during Phase 2. PFS may cause minor delays during key generation.	enable
phase1name <gateway_name>	Enter a phase 1 gateway configuration name. You must add the phase 1 gateway definition to the FortiGate configuration before it can be cross-referenced.	Null.

Variable	Description	Default
proposal <encryption_combination>	Enter a minimum of one and a maximum of three encryption-message digest combinations (for example, 3des-md5). The remote peer must be configured to use at least one of the proposals that you define. Use a space to separate the combinations. You can enter any encryption-message digest combination except null-null. Here is an explanation of the abbreviated encryption algorithms: • null— Do not use an encryption algorithm. • des — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3des — Triple-DES, in which plain text is encrypted three times by three keys. • aes128 — A 128-bit block algorithm that uses a 128-bit key. • aes192 — A 128-bit block algorithm that uses a 192-bit key. • aes256 — A 128-bit block algorithm that uses a 256-bit key. You can enter any of the following message digests to check the authenticity of messages during an encrypted session: • null — Do not use a message digest. • md5 — Message Digest 5, the hash algorithm developed by RSA Data Security. • sha1— Secure Hash Algorithm 1, which produces a 160-bit message digest. • sha256 — Secure Hash Algorithm 2, which produces a 256-bit message digest.	aes128-sha1 3des-sha1
protocol <protocol_integer>	This field is available when selector is set to specify. Enter the IP protocol number for the service. The range is 1 to 255. To specify all services, type 0.	0
replay {disable | enable}	Optionally, enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPSec packets and replays them back into the tunnel. Enable replay detection to check the sequence number of every IPSec packet to see if it has been received before. If packets arrive out of sequence, the FortiGate units discards them. You can configure the FortiGate unit to send an alert email when it detects a replay packet. See “alertemail” on page 67.	enable
route-overlap {overlap_option}	Specify how FortiGate unit handles multiple dialup users with the same IP source address. Set overlap_option to one of the following: allow — allow overlapping routes use-new — delete the old route and add the new route use-old — use the old route and do not add the new route	use-new
selector-match <match_type>	The peer’s IPSec selectors are compared to FortiGate phase 2 selectors, which are any of src-start-ip / src-end-ip, src-subnet, dst-subnet, dst-start-ip / dst-end-ip. The match_type value can be one of: exact — peer’s selector must match exactly subset — peer’s selector can be a subset of this selector auto — use exact or subset match as needed (default) Note: This field is configured automatically when upgrading a FortiOS version 2.80 VPN to version 3.0. You should not set this field when configuring a new VPN.	auto
single-source {disable | enable}	Enable if src-addr-type is name and hosts on the internal network will initiate communication sessions with remote dialup clients.	disable

Variable	Description	Default
src-addr-type <ip_source_name>	If the FortiGate unit is a dialup server, enter the type of source address that corresponds to the local sender(s) or network behind the FortiGate dialup server: • To specify the IP address of a server or host, type ip. Enter the IP address using the src-start-ip field. • To specify a range of IP addresses, type range. Enter the starting and ending addresses using the src-start-ip and src-end-ip fields. • To specify a network address, type subnet. Enter the network address using the src-subnet field. • To specify a firewall address or address group, type name. Enter the address or address group name using the src-name field. You must also select the name option for dst-addr-type. This option is intended for users upgrading VPN configurations created using FortiOS 2.80. For new VPNs that use firewall addresses or address groups as selectors, interface mode VPNs are recommended. If the FortiGate unit is a dialup client, src-addr-type must refer to the server(s), host(s), or private network behind the FortiGate dialup client.	subnet
src-end-ip <address_ipv4>	This field is available when src-addr-type is set to range. Enter the highest source IP address in the range of IP addresses.	0.0.0.0
src-name <address_name>	This field is available when src-addr-type is set to name. Enter the name of a firewall address or address group.	No default.
src-port <source_port_number>	If the FortiGate unit is a dialup server, enter the port number that the FortiGate dialup server uses to transport traffic related to the specified service (see protocol). If the FortiGate unit is a dialup client, enter the port number that the FortiGate dialup client uses to transport traffic related to the specified service. The src-port range is 1 to 65535. To specify all ports, type 0.	0
src-start-ip <address_ipv4>	This field is available when src-addr-type is set to range. Enter the lowest source IP address in the range of IP addresses.	0.0.0.0
src-subnet <address_ipv4mask>	If the FortiGate unit is a dialup server, enter the IP address and network mask that identifies the private network behind the FortiGate dialup server. If the FortiGate unit is a dialup client, enter the IP address and network mask that identifies the private network behind the FortiGate dialup client.	0.0.0.0 0.0.0.0
use-natip {enable | disable}	By default, when outbound NAT is used, the FortiGate unit public interface IP address is the source selector. If you disable use-natip, the source selector is as specified in src-start-ip / src-end-ip or src-subnet. Note: This field is configured automatically when upgrading a FortiOS version 2.80 VPN to version 3.0. You should not set this field when configuring a new VPN.	enable

Example

Use the following command to add a tunnel-mode phase 2 configuration with the following characteristics:

- Name: New_Tunnel
- Phase 1 name: Simple_GW
- Encryption and authentication proposal: 3des-sha1 aes256-sha1 des-md5
- Keylife type: seconds
- Keylife seconds: 18001
- Diffie-Hellman group: 2

- Replay detection: `enable`
- Perfect forward secrecy: `enable`
- Keepalive: `enable`

```
config vpn ipsec phase2
  edit New_Tunnel
    set phase1name Simple_GW
    set proposal 3des-sha1 aes256-sha1 des-md5
    set keylife-type seconds
    set keylifeseconds 18001
    set dhgrp 2
    set replay enable
    set pfs enable
    set keepalive enable
  end
```

History

FortiOS v2.80	Revised
FortiOS v2.80 MR3	`concentrator` field available in NAT/Route mode only.
FortiOS v2.80 MR7	`wildcardid` field removed. `selector` field and associated `srcaddr`, `dstaddr`, `protocol`, `srcport`, and `dstport` fields added. `single-source` field added.
FortiOS v3.0	Replaced underscore character in `keylife-type` field with a hyphen. Removed `bindtoif`, `concentrator`, `internetbrowsing`, `selector`, `dstaddr`, `dstport`, `srcaddr`, and `srcport` fields. Added `dst-addr-type`, `dst-port`, `dst-subnet`, `dst-end-ip`, `dst-start-ip`, `src-addr-type`, `src-port`, `src-subnet`, `src-end-ip`, and `src-start-ip` fields.
FortiOS v3.0 MR5	Removed `null-null` option from `proposal` field.
FortiOS v4.0.0	`add-route` field added. Changed default value of `proposal` to `aes128-sha1 3des-sha1`. Changed default value of `pfs` and `replay` to `enable`.

Related topics

- vpn ipsec phase1
- alertemail setting
- alertemail setting
- firewall policy, policy6

ipsec phase2-interface

Use this command to add a phase 2 configuration for a route-based (interface mode) IPSec tunnel or edit an existing interface-mode phase 2 configuration. This command is available only in NAT/Route mode.

Syntax

```
config vpn ipsec phase2-interface
  edit <tunnel_name>
    set auto-negotiate {enable | disable}
    set dhcp-ipsec {disable | enable}
    set dhgrp {1 | 2 | 5 | 14}
    set dst-addr-type <type>
    set dst-end-ip <address_ipv4>
    set dst-end-ip6 <address_ipv6>
    set dst-name <address_name>
    set dst-port <destination_port_number>
    set dst-start-ip <address_ipv4>
    set dst-start-ip6 <address_ipv6>
    set dst-subnet <address_ipv4mask>
    set dst-subnet6 <address_ipv6mask>
    set keepalive {disable | enable}
    set keylife-type <keylife_type>
    set keylifekbs <kb_integer>
    set keylifeseconds <seconds>
    set pfs {disable | enable}
    set phase1name <gateway_name>
    set proposal <encryption_combination>
    set protocol <protocol_integer>
    set replay {disable | enable}
    set route-overlap {overlap_option}
    set single-source {disable | enable}
    set src-addr-type <ip_source_name>
    set src-end-ip <address_ipv4>
    set src-end-ip6 <address_ipv6>
    set src-name <address_name>
    set src-port <source_port_number>
    set src-start-ip <address_ipv4>
    set src-start-ip6 <address_ipv6>
    set src-subnet <address_ipv4mask>
    set src-subnet6 <address_ipv6mask>
  end
```

Note: The `phase1name` field is required. All other fields are optional.

Variable	Description	Default
`edit <tunnel_name>`	Enter a name for the phase 2 tunnel configuration.	No default.
`auto-negotiate {enable | disable}`	Enable to negotiate the phase 2 security association (SA) automatically, even if there is no traffic. This repeats every five seconds until it succeeds. You can use this option on a dialup peer to ensure that the tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the tunnel does not exist until the dialup peer initiates traffic.	disable
`dhcp-ipsec {disable | enable}`	This field is available when `phase1name` names a dialup gateway configuration. This field is not available if `phase1name` names a configuration that enables `mode-cfg`. Enable `dhcp-ipsec` if the FortiGate unit acts as a dialup server and FortiGate DHCP relay will be used to assign VIP addresses to FortiClient dialup clients. The DHCP relay parameters must be configured separately. If you configure the DHCP server to assign IP addresses based on RADIUS user group attributes, you must also set the `peertype` to `dialup` and specify the `usrgrp` in vpn ipsec phase1. For information about how to configure a DHCP server on a FortiGate interface, see "system dhcp server" on page 410. For information about FortiGate DHCP relay, see "system interface" on page 448. If the FortiGate unit acts as a dialup server and you manually assigned FortiClient dialup clients VIP addresses that match the network behind the dialup server, select Enable to cause the FortiGate unit to act as a proxy for the dialup clients.	`disable`
`dhgrp {1 | 2 | 5 | 14}`	Type 1, 2, 5, or 14 to select the Diffie-Hellman group to propose for Phase 2 of the IPSec VPN connection. Both VPN peers must use the same DH Group.	5
`dst-addr-type <type>`	Enter the type of destination address that corresponds to the recipient(s) or network behind the remote VPN peer or FortiGate dialup client: • To specify the IPv4 IP address of a server or host, type `ip`. Enter the IP address using the `dst-start-ip` field. • To specify the IPv6 IP address of a server or host, type `ip6`. Enter the IP address using the `dst-start-ip6` field. • To specify a range of IPv4 IP addresses, type `range`. Enter the starting and ending addresses using the `dst-start-ip` and `dst-end-ip` fields. • To specify a range of IPv6 IP addresses, type `range6`. Enter the starting and ending addresses using the `dst-start-ip6` and `dst-end-ip6` fields. • To specify an IPv4 network address, type `subnet`. Enter the network address using the `dst-subnet` field. • To specify an IPv6 network address, type `subnet6`. Enter the network address using the `dst-subnet` field. • To specify an address defined in a firewall address or address group, type `name`. Enter the address name using the `dst-name` field. You must also select the `name` option for `src-addr-type`. This is available only for IPv4 addresses. This field is not available if `phase1name` names a configuration that enables `mode-cfg`.	`subnet`
`dst-end-ip <address_ipv4>`	This field is available when `dst-addr-type` is set to `range`. This field is not available if `phase1name` names a configuration that enables `mode-cfg`. Enter the highest destination IP address in the range of IP addresses.	`0.0.0.0`

Variable	Description	Default
dst-end-ip6 <address_ipv6>	This field is available when dst-addr-type is set to range6. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the highest destination IP address in the range of IP addresses.	::
dst-name <address_name>	This field is available when dst-addr-type is set to name. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the firewall address or address group name.	No default.
dst-port <destination_port_number>	Enter the port number that the remote VPN peer or FortiGate dialup client uses to transport traffic related to the specified service (see protocol). The range is 1 to 65535. To specify all ports, type 0. This field is not available if phase1name names a configuration that enables mode-cfg.	0
dst-start-ip <address_ipv4>	This field is available when dst-addr-type is set to range. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the lowest destination IP address in the range of IP addresses.	0.0.0.0
dst-start-ip6 <address_ipv6>	This field is available when dst-addr-type is set to range6. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the lowest destination IP address in the range of IP addresses.	::
dst-subnet <address_ipv4mask>	Enter the IPv4 IP address and network mask that identifies the private network behind the remote VPN peer or FortiGate dialup client. This field is not available if phase1name names a configuration that enables mode-cfg.	0.0.0.0 0.0.0.0
dst-subnet6 <address_ipv6mask>	Enter the IPv6 IP address and network mask that identifies the private network behind the remote VPN peer or FortiGate dialup client. This field is not available if phase1name names a configuration that enables mode-cfg.	::/0
keepalive {disable | enable}	Enable to automatically negotiate a new phase 2 security association (SA) before the current SA expires, keeping the tunnel up. Otherwise, a new SA is negotiated only if there is traffic.	disable
keylife-type <keylife_type>	Set when the phase 2 key expires. When the key expires, a new key is generated without interrupting service. • To make the key expire after a period of time has expired and after an amount of data is transmitted, type both. • To make the key expire after an amount of data is transmitted, type kbs. Use the keylifekbs field to set the amount of data that is transmitted. • To make the key expire after a number of seconds elapses, type seconds. Use the keylifeseconds field to set the amount of time that elapses.	seconds
keylifekbs <kb_integer>	This field is available when keylife-type is set to kbs or both. Set the number of KBytes of data to transmit before the phase 2 key expires. The range is 5120 to 99999 KBytes.	5120
keylifeseconds <seconds>	This field is available when keylife-type is set to seconds or both. Set the number of seconds to elapse before the phase 2 key expires. seconds can be 120 to 172800 seconds.	1800

Variable	Description	Default
pfs {disable | enable}	Optionally, enable or disable perfect forward secrecy (PFS). PFS ensures that each key created during Phase 2 is unrelated to keys created during Phase 1 or to other keys created during Phase 2. PFS may cause minor delays during key generation.	enable
phase1name <gateway_name>	Enter a phase 1 gateway configuration name. You must add the phase 1 gateway definition to the FortiGate configuration before it can be cross-referenced.	Null.
proposal <encryption_combination>	Enter a minimum of one and a maximum of three encryption-message digest combinations (for example, 3des-md5). The remote peer must be configured to use at least one of the proposals that you define. Use a space to separate the combinations. You can enter any encryption-message digest combination except null-null. Here is an explanation of the abbreviated encryption algorithms: • null — Do not use an encryption algorithm. • des — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • 3des — Triple-DES, which encrypts data three times by three keys. • aes128 — A 128-bit block algorithm that uses a 128-bit key. • aes192—- A 128-bit block algorithm that uses a 192-bit key. • aes256 — A 128-bit block algorithm that uses a 256-bit key. You can enter any of the following message digests to check the authenticity of messages during an encrypted session: • null — Do not use a message digest. • md5 — Message Digest 5, the hash algorithm developed by RSA Data Security. • sha1 — Secure Hash Algorithm 1, which produces a 160-bit message digest. • sha256 — Secure Hash Algorithm 2, which produces a 256-bit message digest.	aes128-sha1 3des-sha1
protocol <protocol_integer>	This field is available when selector is set to specify. Enter the IP protocol number for the service. The range is 1 to 255. To specify all services, type 0.	0
replay {disable | enable}	Optionally, enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPSec packets and replays them back into the tunnel. Enable replay detection to check the sequence number of every IPSec packet to see if it has been received before. If packets arrive out of sequence, the FortiGate units discards them. You can configure the FortiGate unit to send an alert email when it detects a replay packet. See “alertemail” on page 67.	enable
route-overlap {overlap_option}	Specify how FortiGate unit handles multiple dialup users with the same IP source address. Set overlap_option to one of the following: • allow — allow overlapping routes • use-new — delete the old route and add the new route • use-old — use the old route and do not add the new route	use-new
single-source {disable | enable}	Enable or disable all FortiClient dialup clients to connect using the same phase 2 tunnel definition.	disable

Variable	Description	Default
src-addr-type <ip_source_name>	If the FortiGate unit is a dialup server, enter the type of source address that corresponds to the local sender(s) or network behind the FortiGate dialup server: • To specify the IPv4 IP address of a server or host, type ip. Enter the IP address using the src-start-ip field. • To specify the IPv6 IP address of a server or host, type ip6. Enter the IP address using the src-start-ip6 field. • To specify a range of IPv4 IP addresses, type range. Enter the starting and ending addresses using the src-start-ip and src-end-ip fields. • To specify a range of IPv6 IP addresses, type range6. Enter the starting and ending addresses using the src-start-ip6 and src-end-ip6 fields. • To specify an IPv4 network address, type subnet. Enter the network address using the src-subnet field. • To specify an IPv6 network address, type subnet6. Enter the network address using the src-subnet6 field. • To specify an address defined in a firewall address or address group, type name. Enter the address name using the src-name field. You must also select the name option for dst-addr-type. This is available only for IPv4 addresses. If the FortiGate unit is a dialup client, src-addr-type must refer to the server(s), host(s), or private network behind the FortiGate dialup client. This field is not available if phase1name names a configuration that enables mode-cfg.	subnet
src-end-ip <address_ipv4>	This field is available when src-addr-type is set to range. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the highest source IP address in the range of IP addresses.	0.0.0.0
src-end-ip6 <address_ipv6>	This field is available when src-addr-type is set to range6. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the highest source IP address in the range of IP addresses.	::
src-name <address_name>	This field is available when src-addr-type is set to name. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the firewall address or address group name.	
src-port <source_port_number>	If the FortiGate unit is a dialup server, enter the port number that the FortiGate dialup server uses to transport traffic related to the specified service (see protocol). If the FortiGate unit is a dialup client, enter the port number that the FortiGate dialup client uses to transport traffic related to the specified service. The src-port range is 1 to 65535. To specify all ports, type 0. This field is not available if phase1name names a configuration that enables mode-cfg.	0
src-start-ip <address_ipv4>	This field is available when src-addr-type is set to range. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the lowest source IP address in the range of IP addresses.	0.0.0.0
src-start-ip6 <address_ipv6>	This field is available when src-addr-type is set to range6. This field is not available if phase1name names a configuration that enables mode-cfg. Enter the lowest source IP address in the range of IP addresses.	::

Variable	Description	Default
src-subnet <address_ipv4mask>	If the FortiGate unit is a dialup server, enter the IPv4 IP address and network mask that identifies the private network behind the FortiGate dialup server. If the FortiGate unit is a dialup client, enter the IP address and network mask that identifies the private network behind the FortiGate dialup client. This field is not available if phase1name names a configuration that enables mode-cfg.	0.0.0.0 0.0.0.0
src-subnet6 <address_ipv6mask>	If the FortiGate unit is a dialup server, enter the IPv6 IP address and network mask that identifies the private network behind the FortiGate dialup server. If the FortiGate unit is a dialup client, enter the IP address and network mask that identifies the private network behind the FortiGate dialup client. This field is not available if phase1name names a configuration that enables mode-cfg.	::/0

Example

Use the following command to add a route-based (interface mode) phase 2 configuration with the following characteristics:

- Name: Interface_Tunnel
- Phase 1 name: Interface_GW
- Encryption and authentication proposal: 3des-sha1 aes256-sha1 des-md5
- Keylife type: seconds
- Keylife seconds: 18001
- Diffie-Hellman group: 2
- Replay detection: enable
- Perfect forward secrecy: enable
- Keepalive: enable

```
config vpn ipsec phase2-interface
  edit Interface_Tunnel
    set phase1name Interface_GW
    set proposal 3des-sha1 aes256-sha1 des-md5
    set keylife-type seconds
    set keylifeseconds 18001
    set dhgrp 2
    set replay enable
    set pfs enable
    set keepalive enable
  end
```

History

FortiOS v3.0	New
FortiOS v3.0 MR3	added src-addr-type name, src-name, dst-addr-type name, dst-name.
FortiOS v3.0 MR5	Removed null-null option from proposal field. Added ip6, range6, subnet6 options to src-addr-type field. Added dst-end-ip6, dst-start-ip6, dst-subnet6, src-end-ip6, src-start-ip6, src-subnet6 fields.

FortiOS v4.0.0	Added `dhcp-ipsec` field. Changed default value of `proposal` to `aes128-sha1 3des-sha1`. Changed default value of `pfs` and `replay` to `enable`.
FortiOS v4.0 MR1	Added information about effect of enabling `mode-cfg` in the corresponding `phase1-interface` configuration.

Related topics

- vpn ipsec phase1-interface
- alertemail setting
- alertemail setting
- firewall policy, policy6

l2tp

Use this command to enable L2TP and specify a local address range to reserve for remote L2TP clients. When a remote L2TP client connects to the internal network through a L2TP VPN, the client is assigned an IP address from the specified range.

L2TP clients must authenticate with the FortiGate unit when a L2TP session starts. To support L2TP authentication on the FortiGate unit, you must define the L2TP users who need access and then add them to a user group. For more information, see “user group” on page 551, “user ldap” on page 555, “user local” on page 558, and “user radius” on page 563.

You need to define a firewall policy to control services inside the L2TP tunnel. For more information, see “firewall” on page 109. When you define the firewall policy:

- Create an “external -> internal” policy.
- Set the source address to match the L2TP address range.
- Set the destination address to reflect the private address range of the internal network behind the local FortiGate unit.
- Set the policy service(s) to match the type(s) of traffic that L2TP users may generate.
- Set the policy action to `accept`.
- Enable NAT if required.

Caution: FortiGate units support L2TP with Microsoft Point-to-Point Encryption (MPPE) encryption only. Later implementations of Microsoft L2TP for Windows use IPSec and require certificates for authentication and encryption. If you want to use Microsoft L2TP with IPSec to connect to a FortiGate unit, the IPSec and certificate elements must be disabled on the remote client. For more information, see the *Disabling Microsoft L2TP for IPSec* article in the Fortinet Knowledge Center.

Syntax

```
config vpn l2tp
  set eip <address_ipv4>
  set sip <address_ipv4>
  set status {disable | enable}
  set usrgrp <group_name>
end
```

Note: You can configure L2TP VPNs on FortiGate units that run in NAT/Route mode. The commands are available in NAT/Route mode only. When you configure an L2TP address range for the first time, you must enter a starting IP address, an ending IP address, and a user group.

Variable	Description	Default
`eip <address_ipv4>`	The ending IP address of the L2TP address range.	`0.0.0.0`
`sip <address_ipv4>`	The starting IP address of the L2TP address range.	`0.0.0.0`
`status {disable | enable}`	Enable or disable L2TP VPN.	`disable`
`usrgrp <group_name>`	This field is available when `status` is set to `enable`. Enter the name of the user group for authenticating L2TP clients. The user group must be added to the FortiGate configuration before it can be specified here. For more information, see “user group” on page 551, “user ldap” on page 555, “user local” on page 558, and “user radius” on page 563.	`Null.`

Example

This example shows how to enable L2TP and set the L2TP address range for the first time using a starting address of `192.168.1.150`, an ending address of `192.168.1.160` and an existing group of L2TP users named `L2TP_users`:

```
config vpn l2tp
  set sip 192.168.1.150
  set eip 192.168.1.160
  set status enable
  set usrgrp L2TP_users
end
```

History

FortiOS v2.80 Revised

Related topics

- user group
- firewall policy, policy6

pptp

Use this command to enable PPTP and specify a local address range to reserve for remote PPTP clients. When a remote PPTP client connects to the internal network through a PPTP VPN, the client is assigned an IP address from the specified range or from the server defined in the PPTP user group.

PPTP clients must authenticate with the FortiGate unit when a PPTP session starts. To support PPTP authentication on the FortiGate unit, you must define the PPTP users who need access and then add them to a user group. For more information, see “user group” on page 551, “user ldap” on page 555, “user local” on page 558, “user radius” on page 563, “user peer” on page 560, and “user peergrp” on page 562.

You need to define a firewall policy to control services inside the PPTP tunnel. For more information, see “firewall” on page 109. When you define the firewall policy:

- Create an “external -> internal” policy.
- Set the source address to match the PPTP address range.
- Set the destination address to reflect the private address range of the internal network behind the local FortiGate unit.
- Set the policy service(s) to match the type(s) of traffic that PPTP users may generate.
- Set the policy action to `accept`.
- Enable NAT if required.

When you intend to use the FortiGate unit as a PPTP gateway, you can select a PPTP client IP from a local address range or use the server defined in the PPTP user group. You select which method to use for IP address retrieval and, in the case of the user group server, provide the IP address and the user group.

The FortiGate unit retrieves the `Framed-IP-Address` (the actual IP address of the client) from the RADIUS accounting start/stop message when `ip-mode` is set to `usrgrp`.

Syntax

```
config vpn pptp
  set eip <address_ipv4>
  set ip-mode {range | usrgrp}
  set local-ip {address_localip}
  set sip <address_ipv4>
  set status {disable | enable}
  set usrgrp <group_name>
end
```

Note: You can configure PPTP VPNs on FortiGate units that run in NAT/Route mode. The commands are available in NAT/Route mode only. When you configure a PPTP address range for the first time, you must enter a starting IP address, an ending IP address, and a user group.

Variable	Description	Default
`eip <address_ipv4>`	The ending address of the PPTP address range.	`0.0.0.0`
`ip-mode {range | usrgrp}`	Select one of: `range` — Assign user IP addresses from the IP address range of configured by `sip` and `eip`. `usrgrp` — Retrieve the IP address from the user group used to authenticate the user. Select the user group in `usrgrp`.	`range`
`local-ip {address_localip}`	Enter the IP address to be used for the peer’s remote IP on the PPTP client side.	`0.0.0.0`
`sip <address_ipv4>`	The starting address of the PPTP IP address range.	`0.0.0.0`

Variable	Description	Default
`status {disable | enable}`	Enable or disable PPTP VPN.	`disable`
`usrgrp <group_name>`	This field is available when `ip-mode` is set to `usrgrp`. Enter the name of the user group for authenticating PPTP clients. The user group must be added to the FortiGate configuration before it can be specified here. For more information, see "user group" on page 551, "user ldap" on page 555, "user local" on page 558, "user radius" on page 563, "user peer" on page 560, and "user peergrp" on page 562	`Null.`

Example

This example shows how to enable PPTP and set the PPTP address range for the first time using a starting address of `192.168.1.100`, an ending address of `192.168.1.130` and an existing group of PPTP users named `PPTP_users`:

```
config vpn pptp
  set sip 192.168.1.100
  set eip 192.168.1.130
  set status enable
  set usrgrp PPTP_users
end
```

This example shows how to enable PPTP and set the IP address from the PPTP user group server.

```
config vpn pptp
  set ip-mode usrgrp
  set local-ip 172.14.12.14
  set status enable
  set usrgrp PPTP_users
end
```

History

FortiOS v2.80	Revised
FortiOS v3.0 MR5	Added links for PKI user and user group (peer and peer group).
FortiOS v4.0	Added information about selecting PPTP IP address from user group. New variables introduced: `ip-mode` and `local-ip`.

Related topics

- user group
- firewall policy, policy6

ssl settings

Use this command to configure basic SSL VPN settings including interface idle-timeout values and SSL encryption preferences. If required, you can also enable the use of digital certificates for authenticating remote clients.

You can optionally specify the IP address of any Domain Name Service (DNS) server and/or Windows Internet Name Service (WINS) server that resides on the private network behind the FortiGate unit. The DNS and/or WINS server will find the IP addresses of other computers whenever a connected SSL VPN user sends an email message or browses the Internet.

Note: You can configure SSL VPNs on FortiGate units that run in NAT/Route mode. The commands are available in NAT/Route mode only.

Syntax

```
config vpn ssl settings
  set algorithm <cipher_suite>
  set auth-timeout <auth_seconds>
  set deflate-compression-level <int>
  set deflate-min-data-size <int>
  set dns-server1 <address_ipv4>
  set dns-server2 <address_ipv4>
  set force-two-factor-auth {enable | disable}
  set force-utf8-login {enable | disable}
  set http-compression {enable | disable}
  set idle-timeout <idle_seconds>
  set portal-heading <caption>
  set reqclientcert {disable | enable}
  set route-source-interface {disable | enable}
  set servercert <server_cert_name>
  set sslv2 {disable | enable}
  set sslv3 {disable | enable}
  set sslvpn-enable {disable | enable}
  set tunnel-ip-pools <pool1_name...pooln_name>
  set url-obscuration {disable | enable}
  set wins-server1 <address_ipv4>
  set wins-server2 <address_ipv4>
end
```

Note: Set the `sslvpn-enable` attribute to `enable` to view all possible settings. The `tunnel-ip-pools` field is required for tunnel-mode access only. All other fields are optional.

When you configure the timeout settings, if you set the authentication timeout (`auth-timeout`) to 0, then the remote client does not have to re-authenticate again unless they log out of the system. In order to fully take advantage of this setting, the value for `idle-timeout` has to be set to 0 also, so the client does not timeout if the maximum idle time is reached. If the `idle-timeout` is not set to the infinite value, the system will log out if it reaches the limit set, regardless of the `auth-timeout` setting.

Variable	Description	Default
`algorithm <cipher_suite>`	This field is available when `sslvpn-enable` is set to enable. Enter one of the following options to determine the level of SSL encryption to use. The web browser on the remote client must be capable of matching the level that you specify: • To use any cipher suite, type `low`. • To use a 128-bit or greater cipher suite, type `default`. • To use a cipher suite that is greater than 128 bits, type `high`.	`default`
`auth-timeout <auth_seconds>`	This field is available when `sslvpn-enable` is set to enable. Enter the period of time (in seconds) to control how long an authenticated connection will remain connected. When this time expires, the system forces the remote client to authenticate again. Range is 10 to 259,200 seconds (3 days). Use the value of 0 to indicate no timeout.	`1500`
`deflate-compression-level <int>`	Set the compression level. Range is 1 (least compression) to 9 (most compression). Higher compression reduces the volume of data but requires more processing time. This field is available when `http-compression` is enabled.	`6`
`deflate-min-data-size <int>`	Set the minimum amount of data that will trigger compression. Smaller amounts are not compressed. Range is 200 to 65 535 bytes. This field is available when `http-compression` is enabled.	`300`
`dns-server1 <address_ipv4>`	Enter the IP address of the primary DNS server that SSL VPN clients will be able to access after a connection has been established. If required, you can specify a secondary DNS server through the `dns-server2` attribute.	`0.0.0.0`
`dns-server2 <address_ipv4>`	Enter the IP address of a secondary DNS server if required.	`0.0.0.0`
`force-two-factor-auth {enable | disable}`	Enable to require PKI (peer) users to authenticate by password in addition to certificate authentication. If this is enabled, only PKI users with two-factor authentication enabled will be able to log on to the SSL VPN.	`disable`
`force-utf8-login {enable | disable}`	Enable to use UTF-8 encoding for the login page. This might be necessary when using LDAP to authenticate users.	`disable`
`http-compression {enable | disable}`	Enable use of compression between the FortiGate unit and the client web browser. You can adjust the fields `deflate-compression-level` and `deflate-min-data-size` to tune performance.	`disable`
`idle-timeout <idle_seconds>`	This field is available when `sslvpn-enable` is set to enable. Enter the period of time (in seconds) to control how long the connection can remain idle before the system forces the remote user to log in again. The range is from 10 to 28800 seconds. Use the value of 0 to indicate no timeout.	`300`
`portal-heading <caption>`	This field is available when `sslvpn-enable` is set to enable. If you want to display a custom caption at the top of the web portal home page, type the message.	`Null.`
`reqclientcert {disable | enable}`	This field is available when `sslvpn-enable` is set to enable. Disable or enable the use of group certificates for authenticating remote clients.	`disable`
`route-source-interface {disable | enable}`	This field is available when `sslvpn-enable` is set to enable. Enable to allow the SSL VPN connection to bypass routing and bind to the incoming interface.	`disable`

Variable	Description	Default
servercert <server_cert_name>	This field is available when sslvpn-enable is set to enable. Enter the name of the signed server certificate that the FortiGate unit will use to identify itself during the SSL handshake with a web browser when the web browser connects to the login page. The server certificate must already be loaded into the FortiGate configuration. If you do not specify a server certificate, the FortiGate unit offers its factory installed (self-signed) certificate from Fortinet to remote clients when they connect.	self-sign
sslv2 {disable | enable}	This field is available when sslvpn-enable is set to enable. Disable or enable SSL version 2 encryption.	disable
sslv3 {disable | enable}	This field is available when sslvpn-enable is set to enable. Disable or enable SSL version 3 encryption.	enable
sslvpn-enable {disable | enable}	Disable or enable remote-client access.	disable
tunnel-ip-pools <pool1_name...pool*n*_name>	Enter the firewall addresses that represent the ranges of IP addresses reserved for remote clients. This field is available when sslvpn-enable is set to enable.	No default.
url-obscuration {disable | enable}	This field is available when sslvpn-enable is set to enable. Enable to encrypt the host name of the url in the display (web address) of the browser for web mode only. This is a requirement for ICSA ssl vpn certification. Also, if enabled, bookmark details are not visible (field is blank.).	disable
wins-server1 <address_ipv4>	Enter the IP address of the primary WINS server that SSL VPN clients will be able to access after a connection has been established. If required, you can specify a secondary WINS server through the wins-server2 attribute.	0.0.0.0
wins-server2 <address_ipv4>	Enter the IP address of a secondary WINS server if required.	0.0.0.0

Example

The following command enables the FortiGate unit to assign virtual IP addresses in the 10.10.10.100 to 10.10.10.105 range to authenticated clients (an IP address range is needed to support tunnel-mode access). The command also sets timeout values for authenticated connections and connection inactivity respectively.

```
config firewall address
  edit SSLVPN_client_range
    set type iprange
    set start-ip 10.10.10.100
    set end-ip 10.10.10.105
  end
config vpn ssl settings
   set sslvpn-enable enable
   set tunnel-ip-pools SSLVPN_client_range
   set auth-timeout 600
   set idle-timeout 1500
end
```

History

FortiOS v3.0 New.

FortiOS v3.0 MR4 Added route-source-interface.

FortiOS v3.0 MR5 Added url-obscuration.

FortiOS v3.0 MR6	Changed values in `auth-timeout` and `idle-timeout` to include infinity setting.
FortiOS v3.0 MR7	If `url-obscuration` is enabled, bookmark details are not visible.
FortiOS v4.0 MR1	Added `force-two-factor-auth`, `force-utf8-login, deflate-compression-level`, `deflate-min-data-size`, `http-compression`. Added `tunnel-ip-pools`, removed `tunnel-startip` and `tunnel-endip`.

Related topics

- system replacemsg sslvpn
- execute vpn sslvpn del-tunnel
- get vpn ssl monitor
- user group
- user peer
- firewall policy, policy6

ssl web host-check-software

Use this command to define security software for selection in the `host-check-policy` field of the `vpn ssl web portal` command.

Syntax

```
config vpn ssl web host-check-software
  edit <software_name>
    set guid <guid>
    set type {av | fw}}
    set version <version_str>
    config check-item-list
      edit <id_int>
        set action {deny | require}
        set md5s <md5_str>
        set target {file | process | registry}
        set type {file | process | registry}
        set version <version-str>
      end
    end
```

Variable	Description	Default
`<software_name>`	Enter a name to identify the software. The name does not need to match the actual application name.	
`set guid <guid>`	Enter the globally unique identifier (GUID) for the host check application. The GUID is usually in the form xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, where each x is a hexadecimal digit. Windows uses GUIDs to identify applications in the Windows Registry.	No default.
`set type {av | fw}}`	Select the software type: antivirus (`av`) or firewall (`fw`). If the software does both, create two entries, one where `type` is `av` and one where `type` is `fw`.	`av`
`set version <version_str>`	Enter the software version.	No default.
`check-item-list` **variables**		
`<id_int>`	Enter an ID number for this entry.	
`set action {deny | require}`	Select one of `require` — If the item is found, the client meets the check item condition. `deny` — If the item is found, the client is considered to not meet the check item condition. Use this option if it is necessary to prevent use of a particular security product.	`require`
`set md5s <md5_str>`	If `type` is `file` or `process`, enter one or more known MD5 signatures for the application executable file.You can use a third-party utility to calculate MD5 signatures or hashes for any file. You can enter multiple signatures to match multiple versions of the application.	
`set target {file | process | registry}`	Enter information as follows: If `type` is `file`, enter the full path to the file. If `type` is `process`, enter the application's executable file name. If `type` is `registry`, enter the registry item.	No default.

Variable	Description	Default
`set type {file | process | registry}`	Select how to check for the application: • `file` — Look for a file. This could be the application's executable file or any other file that would confirm the presence of the application. Set `target` to the full path to the file. Where applicable, you can use environment variables enclosed in percent (%) marks. For example, `%ProgramFiles%\Fortinet\FortiClient\FortiClient.exe`. • `process` — Look for the application as a running process. Set `target` to the application's executable file name. • `registry` — Search for a Windows Registry entry. Set `target` to the registry item, for example `HKLM\SOFTWARE\Fortinet\FortiClient\Misc`.	`file`
`set version <version-str>`	Enter the version of the application.	No default.

History

FortiOS v4.0 MR1 New.

Related topics

- vpn ssl web portal

ssl web portal

The SSL VPN Service portal allows you to access network resources through a secure channel using a web browser. FortiGate administrators can configure log in privileges for system users and which network resources are available to the users, such as HTTP/HTTPS, telnet, FTP, SMB/CIFS, VNC, RDP and SSH.

The portal configuration determines what the system user sees when they log in to the FortiGate. Both the system administrator and the system user have the ability to customize the SSL VPN portal.

There are three pre-defined default web portal configurations available:

- *full-access*: Includes all widgets available to the user - *Session Information*, *Connection Tool*, *Bookmarks*, and *Tunnel Mode*.
- *tunnel-access*: Includes *Session Information* and *Tunnel Mode* widgets.
- *web-access*: Includes *Session Information* and *Bookmarks* widgets.

These pre-defined portal configurations can be edited, including their names.

Syntax

```
config vpn ssl web portal
  edit <portal_name>
    set allow-access <allow_access>
    set allow-user-bookmark {enable | disable}
    set cache-cleaner {disable | enable}
    set heading <str_heading>
    set host-check {av | av-fw | custom | fw | none}
    set host-check-interval <seconds>
    set host-check-policy <hcpolicy_name>
    set limit-user-logins {enable | disable}
    set os-check {disable | enable}
    set page-layout <double-column | single-column>
    set redir-url <redir_url>
    set theme <blue | gray | orange>
    set virtual-desktop {disable | enable}
    config os-check-list {windows-2000 | windows-vista | windows-xp}
      set action {allow | check-up-to-date | deny}
      set latest-patch-level {disable | 0 - 255}
      set tolerance {tolerance_num}
    end
    config widget
      edit id <widget_id>
        set name <name_str>
        set type <widget_type>
        set column <column_number>
        set collapse {disable | enable}
        set allow-apps <service_type_access>
        set tunnel-status {disable | enable}
        set split-tunneling {disable | enable}
        set split-tunneling-routing-address <address_name>
        set ip-mode {range | usrgrp}
        set ip-pools {<pool1_name> .. <pooln_name>}
        config bookmarks
          edit name <bookmark_name>
            set apptype <service_type>
            set url <target_ip>
```

```
            set host <host_name>
            set folder <folder_name>
            set description <description_txt>
            set sso {disable | auto | static}
            config form-data
              edit <id_int>
                set name <fieldname_str>
                set value <value_str>
              end
            end
          end
        end
      end
    end
end
```

Variable	Description	Default
`edit <str_portal_name>`	Enter a name for the portal. Three pre-defined web portal configurations exist: `full-access`, `tunnel-access`, and `web-access`.	No default.
`allow-access <allow_access>`	Allow access to SSL VPN applications. • Type `ftp` for FTP services. • Type `ping` for pinging hosts. • Type `rdp` for Windows Terminal services. • Type `smb` for SMB/CIFS (Windows file share) services. • Type `ssh` for SSH services. • Type `telnet` for telnet services. • Type `vnc` for VNC services. • Type `web` for HTTP and/or HTTPS services.	No default.
`allow-user-bookmark {enable | disable}`	Allow web portal users to create their own bookmarks.	`enable`
`cache-cleaner {disable | enable}`	Enable the FortiGate unit to remove residual information from the remote client computer just before the SSL VPN session ends. This is done with a downloaded ActiveX control or	`disable`
`heading <str_heading>`	Enter the caption that appears at the top of the web portal home page.	null
`host-check {av | av-fw | custom | fw | none}`	Select the type of host checking to perform on endpoints: **`av`** — Check for antivirus software recognized by the Windows Security Center. **`av-fw`** — Check for both antivirus and firewall software recognized by the Windows Security Center. **`custom`** — Check for the software defined in `host-check-policy`. **`fw`** — Check for firewall software recognized by the Windows Security Center. **`none`** — Do not perform host checking.	`none`
`host-check-interval <seconds>`	Enter how often to recheck the host. Range is every 120 seconds to 259 200 seconds. Enter 0 to not recheck the host during the session. This is not available if `host-check` is `none`.	0
`host-check-policy <hcpolicy_name>`	Select the specific host check software to look for. These applications are defined in the vpn ssl web host-check-software command. This field is available when `host-check` is `custom`.	null
`limit-user-logins {enable | disable}`	Enable to allow each user one SSL VPN session at a time.	`disable`

Variable	Description	Default
os-check {disable | enable}	Enable the FortiGate unit to determine what action to take depending on what operating system the client has.	disable
page-layout <double-column | single-column>	Select the number of columns in the portal display.	single-column
redir-url <redir_url>	Enter the URL of the web page which will enable the FortiGate unit to display a second HTML page in a popup window when the web portal home page is displayed. The web server for this URL must reside on the private network behind the FortiGate unit.	null
theme <blue | gray | orange>	Select the portal display theme (color).	blue
virtual-desktop {disable | enable}	Enable the SSL VPN virtual desktop client application. If set to enable on the client, attempts to connect via SSL VPN are refused.	disable
config os-check-list variables	Available when set os-check is set to check-up-to-date.	
action {allow | check-up-to-date | deny}	Specify how to perform the patch level check. • allow - any level is permitted • check-up-to-date - some patch levels are permitted, make selections for latest-patch-level and tolerance • deny - do not permit access for any version of this OS	allow
latest-patch-level {disable | 0 - 255}	Specify the latest allowed patch level. Available when action is set to enable.	Win2000: 4 WinXP: 2
tolerance {tolerance_num}	Specify the lowest allowable patch level tolerance. Equals latest-patch-level minus tolerance and above. Available when action is check-up-to-date.	0
Widget variables		
id <widget_id>	Enter the unique ID number of the widget.	No default.
name <name_str>	Enter the name for the widget. Maximum 36 characters.	null
type <widget_type>	Enter the type of widget: bookmark, info, tool or tunnel.	bookmark
column <column_number>	Enter the number of columns in the widget display: one or two. This is available if page-layout is double-column.	one
collapse {disable | enable}	Enable the widget to expand in the web portal view. Allows user to make changes to the widget view/configuration.	disable
allow-apps <service_type_access>	If type is bookmark, select the types of bookmarks the user can create. If type is tool, select the types of services that the user can access with this widget. • Type ftp for FTP services. • Type rdp for Windows Terminal services. • Type smb for SMB/CIFS (Windows file share) services. • Type ssh for SSH services. • Type telnet for telnet services. • Type vnc for VNC services. • Type web for HTTP and/or HTTPS services.	No default.
tunnel-status {disable | enable}	Enable the ability of the FortiGate unit to configure SSL VPN tunnel setup for users. Applicable to tunnel widget only.	disable
split-tunneling {disable | enable}	Enable split tunneling. Split tunneling ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route. Available only if tunnel-status is enabled.	disable

Variable	Description	Default
split-tunneling-routing-address <address_name>	Enter the firewall addresses for the destinations that clients will reach through the SSL VPN. The client's split-tunneling configuration will ensure that the tunnel is used for these destinations only. This is available when split-tunneling is enabled.	No default.
ip-mode {range | usrgrp}	Select the mode by which the IP address is assigned to the user: Available only if tunnel-status is enabled.	range
ip-pools {<pool1_name> .. <pooln_name>}	Enter the names of the IP pools (firewall addresses) that represent IP address ranges reserved for tunnel-mode SSL VPN clients. This is available only if tunnel-status is enabled.	
Bookmarks variables Note: config bookmarks is available only when widget type is bookmark.		
name <bookmark_name>	Enter the unique name of the bookmark. Maximum 36 characters.	null
apptype <service_type>	Enter the identifier of the service to associate with the bookmark: • Type ftp for FTP services. • Type rdp for Windows Terminal services. • Type smb for SMB/CIFS (Windows file share) services. • Type ssh for SSH services. • Type telnet for telnet services. • Type vnc for VNC services. • Type web for HTTP and/or HTTPS services.	web
url <target_ip>	Enter the URL of the web page, if apptype is web.	No default.
host <host_name>	Enter the host name, if apptype is telnet or rdp. Maximum 36 characters.	No default.
folder <folder_name>	Enter the remote folder name, if apptype is smb or ftp. The folder name must include the server name, //172.20.120.103/myfolder, for example.	No default.
description <description_txt>	Enter a description of the bookmark. Maximum 129 characters.	null
sso {disable | auto | static}	A Single Sign-On (SSO) bookmark automatically enters the login credentials for the bookmark destination. Select one of: **disable** — This is not an SSO bookmark. **auto** — Use the user's SSL VPN credentials for login. **static** — Use the login credentials defined below.	disable
config field-data **variables**	These fields are available when sso is static.	
name <fieldname_str>	Enter a required login page field name, "User Name" for example.	No default.
value <value_str>	Enter the value to enter in the field identified by name. If you are an administrator configuring a bookmark for users: • Enter %usrname% to represent the user's SSL VPN user name. Enter %passwd% to represent the user's SSL VPN password.	No default.

History

FortiOS v4.0 New.

FortiOS v4.0 MR1 Added host-check, host-check-policy, host-check-interval, limit-user-logins, ip-pools, sso, split-tunneling-routing-address.
layout changed to page-layout.
Removed client-check, client-check-type, start-ip, end-ip.
Changed cache-clean to cache-cleaner.

Related topics

- vpn ssl settings
- vpn ssl web host-check-software

ssl web virtual-desktop-app-list

Use this command to create a list of either allowed or blocked applications which you then select when you configure the virtual desktop.

Syntax

```
config vpn ssl web virtual-desktop-app-list
  edit <applist_name>
    set set action {allow | block}
    config apps
      edit <app_name>
        set md5s <md5_str>
      end
    end
  end
```

Variable	Description	Default
<applist_name>	Enter a name for the application control list.	
set action {allow | block}	Set the action for this application control list: allow — Allow the applications on this list and block all others. block — Block the applications on this list and allow all others	allow
<app_name>	Enter the name of the application to be added to the application control list. This can be any name and does not have to match the official name of the application.	
set md5s <md5_str>	Enter one or more known MD5 signatures (space-separated) for the application executable file.You can use a third-party utility to calculate MD5 signatures or hashes for any file. You can enter multiple signatures to match multiple versions of the application.	No default.

History

FortiOS v4.0 MR1 New.

Related topics

- vpn ssl web portal

wanopt

Use these commands to configure FortiGate WAN optimization.

For more information about WAN optimization, see the *FortiGate WAN Optimization, Web Cache, and Web Proxy User Guide*.

auth-group

Use this command to configure WAN optimization authentication groups. Add authentication groups to support authentication and secure tunneling between WAN optimization peers.

Syntax

```
config wanopt auth-group
  edit <auth_group_name>
    set auth-method {cert | psk}
    set cert <certificate_name>
    set peer <peer_host_id>
    set peer-accept {any | defined | one}
    set psk <preshared_key>
  end
```

Variable	Description	Default
`edit <auth_group_name>`	Enter a name for the authentication group.	
`auth-method {cert | psk}`	Specify the authentication method for the authentication group. Enter `cert` to authenticate using a certificate. Enter `psk` to authenticate using a preshared key.	cert
`cert <certificate_name>`	If `auth-method` is set to `cert`, select the local certificate to be used by the peers in this authentication group. The certificate must be a local certificate added to the FortiGate unit using the `config vpn certificate local` command. For more information, see "vpn certificate local" on page 574.	
`peer <peer_host_id>`	If `peer-method` is set to `one` select the name of one peer to add to this authentication group. The peer must have been added to the FortiGate unit using the `config wanopt peer` command.	
`peer-accept {any | defined | one}`	Specify whether the authentication group can be used for `any` peer, only the `defined` peers that have been added to the FortiGate unit configuration, or just `one` peer. If you specify one use the `peer` field to add the name of the peer to the authentication group.	any
`psk <preshared_key>`	If `auth-method` is set to `psk` enter a preshared key to be used for the authentication group.	

Example

This example shows how to add an authentication group named `auth_grp_1` that uses a certificate named `Example_Cert` and can be used to authenticate all peers added to the FortiGate unit configuration

```
config wanopt auth-group
  edit auth_grp_1
    set auth-method cert
    set cert Example_Cert
    set peer-accept defined
  end
```

History

FortiOS v4.0 New.

Related commands

- wanopt cache-storage
- wanopt peer
- wanopt rule
- wanopt settings
- wanopt ssl-server
- wanopt storage
- wanopt webcache

cache-storage

Using the `execute scsi-dev storage` command you can add multiple WAN optimization storages and then use the `config wanopt cache-storage` command to configure the storages to use for byte caching and web caching. A storage defines the maximum size of the byte caching or web caching database added to the storage.

Unless you have special requirements, you do not need to change `cache-storage` settings unless you use more than one SCSI device for WAN optimization.

You can use the `show wanopt storage` command to view the WAN optimization storages that you have added using the `execute scsi-dev storage` command. You can also use the `config wanopt storage` command to change the storage sizes.

For more information about the `execute scsi-dev` command, see "execute scsi-dev" on page 735.

Syntax

```
config wanopt cache-storage
  set byte-cache-storage <storage_name_str>
  set web-cache-storage <storage_name_str>
end
```

Variable	Description	Default
`byte-cache-storage <storage_name_str>`	Select the WAN optimization storage to use for byte caching.	default
`web-cache-storage <storage_name_str>`	Select the WAN optimization storage to use for web caching.	default

Example

Enter the following commands to configure web caching to use a storage called `web_cache_sto` and byte caching to use a storage called `byte_cache_sto`.

```
config wanopt cache-storage
  set web-cache-storage web_cache_sto
  set byte-cache-storage byte_cache_sto
end
```

History

FortiOS v4.0 New.

Related commands

- execute scsi-dev
- wanopt auth-group
- wanopt peer
- wanopt rule
- wanopt settings
- wanopt ssl-server
- wanopt storage
- wanopt webcache

peer

Add WAN optimization peers to a FortiGate unit to identify the FortiGate units that the local FortiGate unit can form WAN optimization tunnels with. A peer consists of a peer name, which is the local host ID of the remote FortiGate unit and an IP address, which is the IP address of the interface that the remote FortiGate unit uses to connect to the local FortiGate unit.

Use the command `config wanopt settings` to add the local host ID to a FortiGate unit.

Syntax

```
config wanopt peer
  edit <peer_name>
    set ip <peer_ip_ipv4>
  end
```

Variable	Description	Default
`edit <peer_name>`	Add the local host ID of the remote FortiGate unit. When the remote FortiGate unit connects to the local FortiGate unit to start a WAN optimization tunnel, the WAN optimization setup request include the remote FortiGate unit local host ID. If the local host ID in the setup request matches a peer added to the local FortiGate unit, then the local FortiGate unit can accept WAN optimization tunnel setup requests from the remote FortiGate unit.	
`ip <peer_ip_ipv4>`	Enter the IP address of the interface that the remote FortiGate unit uses to connect to the local FortiGate unit. Usually this would be the IP address of the interface connected to the WAN.	0.0.0.0

Example

Use the following commands to add three peers.

```
config wanopt peer
  edit Wan_opt_peer_1
    set ip 172.20.120.100
  next
  edit Wan_opt_peer_2
    set ip 172.30.120.100
  next
  edit Wan_opt_peer_3
    set ip 172.40.120.100
  end
```

History

FortiOS v4.0 New.

Related commands

- wanopt auth-group
- wanopt cache-storage
- wanopt rule
- wanopt settings
- wanopt ssl-server
- wanopt storage, wanopt webcache

rule

WAN optimization uses rules to select traffic to be optimized. But, before WAN optimization rules can accept traffic, the traffic must be accepted by a FortiGate firewall policy. All sessions accepted by a firewall policy that also match a WAN optimization rule are processed by WAN optimization.

To configure WAN optimization you add WAN optimization rules to the FortiGate units at each end of the tunnel. Similar to firewall policies, when the FortiGate unit receives a connection packet, it analyzes the packet's source address, destination address, and service (by destination port number), and attempts to locate a matching WAN optimization rule that decides how to optimize the traffic over WAN.

The FortiGate unit applies firewall policies to packets before WAN optimization rules. A WAN optimization rule is applied to a packet only after the packet is accepted by a firewall policy.

Syntax

```
config wanopt rule
  edit <index_int>
    set auth-group <auth_group_name>
    set auto-detect {active | off | passive}
    set byte-caching {disable | enable}
    set dst-ip <address_ipv4>[-<address-ipv4>]
    set mode {full | webcache-only}
    set peer <peer_name>
    set port <port_int>[-<port-int>]
    set proto {cifs | ftp | http | mapi | tcp}
    set secure-tunnel {disable | enable}
    set src-ip <address_ipv4>[-<address-ipv4>]
    set ssl {disable | enable}
    set status {disable | enable}
    set transparent {disable | enable}
    set tunnel-non-http {disable | enable}
    set tunnel-sharing {express-shared | private | shared}
    set unknown-http-version {best-effort | reject | tunnel}
    set webcache {disable | enable}
  end
```

Variable	Description	Default
`edit <index_int>`	Enter the unique ID number of this rule.	
`auth-group <auth_group_name>`	Select an authentication group to be used by this rule. Select an authentication group if you want the client and server FortiGate units that use this rule to authenticate with each other before starting a WAN optimization tunnel. You must add the same authentication group to the client and server FortiGate units. The authentication group should have the same name of both FortiGate units and use the same pre-shared key or the same certificate. You can add an authentication group to rules with `auto-detect` set to `off` or `active`. An authentication group is required if you enable `secure-tunnel` for the rule.	

Variable	Description	Default
auto-detect {active | off | passive}	Specify whether the rule is an active (client) rule, a passive (server) rule or if auto-detect is off. If auto-detect is off the rule can be a peer to peer rule or a web cache only rule. • For an active (client) rule you must specify all of the WAN optimization features to be applied by the rule. This includes byte-caching, ssl, secure-tunnel, and proto. • A passive (server) rule uses the settings in the active rule on the client FortiGate unit to apply WAN optimization settings. You can also enable webcache for a passive rule. • If auto-detect is off, the rule configuration must include all required WAN optimization features and you must add one peer to the rule.	off
byte-caching {disable | enable}	Enable or disable WAN optimization byte caching for the traffic accepted by this rule. Byte caching is a WAN optimization technique that reduces the amount of data that has to be transmitted across a WAN by caching file data to serve it later as required. Byte caching is available for all protocols. You can enable byte caching for active rules or if auto-detect is off.	enable
dst-ip <address_ipv4>[-<address-ipv4>]	Enter the destination IP address or address range for the rule. Enter a single IP address or the start and end of the IP address range separated by a hyphen. Only packets whose destination address header contains an IP address matching this IP address or address range will be accepted by and subject to this rule.	0.0.0.0
mode {full | webcache-only}	Configure the rule to apply all selected WAN optimization features or just web caching to traffic matched by the rule.	full
peer <peer_name>	Add a peer to the rule. You can only add a peer if auto-detect is off.	(null)
port <port_int>[-<port-int>]	Enter a single port number or port number range for the rule. Only packets whose destination port number matches this port number or port number range will be accepted by and subject to this rule.	0
proto {cifs | ftp | http | mapi | tcp}	Select cifs, ftp, http, or mapi to have the rule apply protocol optimization for one these protocols. Select tcp if the WAN optimization tunnel accepts packets that use more than one protocol or that do not use the CIFS, FTP, HTTP, or MAPI protocol.	http
secure-tunnel {disable | enable}	Enable or disable using AES-128bit-CBC SSL to encrypt and secure the traffic in the WAN optimization tunnel. The FortiGate units use FortiASIC acceleration to accelerate SSL decryption and encryption of the secure tunnel. The secure tunnel uses the same TCP port as a non-secure tunnel (TCP port 7810). You can configure secure-tunnel if auto-detect is set to active or off. If you enable secure-tunnel you must also add an auth-group to the rule.	disable
src-ip <address_ipv4>[-<address-ipv4>]	Enter the source IP address or address range for the rule. Enter a single IP address or the start and end of the IP address range separated by a hyphen. Only packets whose source address header contains an IP address matching this IP address or address range will be accepted by and subject to this rule.	0.0.0.0

Variable	Description	Default
`ssl {disable | enable}`	Enable or disable applying SSL offloading for HTTPS traffic. You use SSL offloading to offload SSL encryption and decryption from one or more HTTP servers. If you enable `ssl`, you should configure the rule to accept SSL-encrypted traffic, usually by configuring the rule to accept HTTPS traffic by setting `port` to 443. If you enable SSL you must also use the `config wanopt ssl-server` command to add an SSL server for each HTTP server that you wan to offload SSL encryption/decryption for. See "wanopt ssl-server" on page 647. You can configure `ssl` if `auto-detect` is set to `active` or `off`.	`disable`
`status {disable | enable}`	Enable or disable the rule.	`enable`
`transparent {disable | enable}`	Enable or disable transparent mode for this rule. If you enable transparent mode, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. Routing on the server network should be able to route traffic with client IP addresses to the FortiGate unit. If you do not select transparent mode, the source address of the packets received by servers is changed to the address of the FortiGate unit interface. So servers appear to receive packets from the FortiGate unit. Routing on the server network is simpler in this case because client addresses are not involved, but the server sees all traffic as coming from the FortiGate unit and not from individual clients.	`enable`
`tunnel-non-http {disable | enable}`	Configure how to process non-HTTP traffic when a rule configured to accept and optimize HTTP traffic accepts a non-HTTP session. This can occur if an application sends non-HTTP traffic using an HTTP destination port. • Select `disable` to drop or tear down non-HTTP sessions accepted by the rule. • Select `enable` to pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied to non-HTTP sessions. You can configure `tunnel-non-http` if `proto` is set to `http` and `auto-detect` is set to `active` or `off`.	`disable`
`tunnel-sharing {express-shared | private | shared}`	Select the tunnel sharing mode for this rule: • Select `express-shared` for rules that accept interactive protocols such as Telnet. • Select `private` for rules that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols. • Select `shared` for rules that accept non-aggressive and non-interactive protocols. You can configure tunnel sharing if `proto` is set to `http` and `auto-detect` is set to `off`. For more information about tunnel sharing, see "About WAN optimization tunnel sharing" on page 643.	`private`

Variable	Description	Default
unknown-http-version {best-effort | reject | tunnel}	Unknown HTTP sessions are HTTP sessions that don't comply with HTTP 0.9, 1.0, or 1.1. Configure unknown-http-version to specify how a rule handles HTTP traffic that does not comply with HTTP 0.9, 1.0, or 1.1. • Select best-effort to assume all HTTP sessions accepted by the rule comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, WAN optimization may not parse it correctly. As a result the FortiGate unit may stop forwarding the session and the connection may be lost. • Select reject to reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1. • Select tunnel to pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied to this HTTP traffic. You can configure unknown-http-version if proto is set to http and auto-detect is set to active or off.	tunnel
webcache {disable | enable}	Enable or disable web caching for this rule. You can enable webcache if proto is set to http and auto-detect set to passive or off.	disable

About WAN optimization tunnel sharing

You can use the tunnel-sharing field to configure tunnel sharing for WAN optimization rules with auto-detect set to off. Tunnel sharing is multiple WAN optimization sessions sharing the same WAN optimization tunnel. Tunnel sharing can improve WAN performance by reducing the number of WAN optimization tunnels between FortiGate units. Fewer tunnels means less data to manage. Also tunnel setup requires more than one exchange of information between the ends of the tunnel. Once the tunnel is set up, each new session that shares the tunnel avoids tunnel setup delays.

Tunnel sharing also uses bandwidth more efficiently by reducing the chances that small packets will be sent down the tunnel. Processing small packets reduces network throughput so reducing the number of small packets improves performance. A shared tunnel can combine all the data from the sessions being processed by the tunnel and send it together. For example, a FortiGate unit is processing five WAN optimization sessions and each session has 100 bytes to send. If these sessions use a shared tunnel, WAN optimization combines the packets from all five sessions into one 500 byte packet. If each session uses its own private tunnel, five 100 byte packets will be sent instead. Each packet also requires a TCP ACK reply. The combined packet in the shared tunnel requires one TCP ACK packet. The separate packets in the private tunnels require 5 TCP ACK packets.

Tunnel sharing is not always recommended. Aggressive and non-aggressive protocols should not share the same tunnel. An aggressive protocol can be defined as a protocol that is able to get more bandwidth than a non-aggressive protocol (the aggressive protocols can "starve" the non-aggressive protocols). HTTP and FTP are considered aggressive protocols. If aggressive and non-aggressive protocols share the same tunnel, the aggressive protocols may take all of the available bandwidth. As a result, the performance of less aggressive protocols could be reduced. To avoid this problem, rules for HTTP and FTP traffic should have their own tunnel. To do this, set tunnel-sharing to private for WAN optimization rules that accept HTTP or FTP traffic.

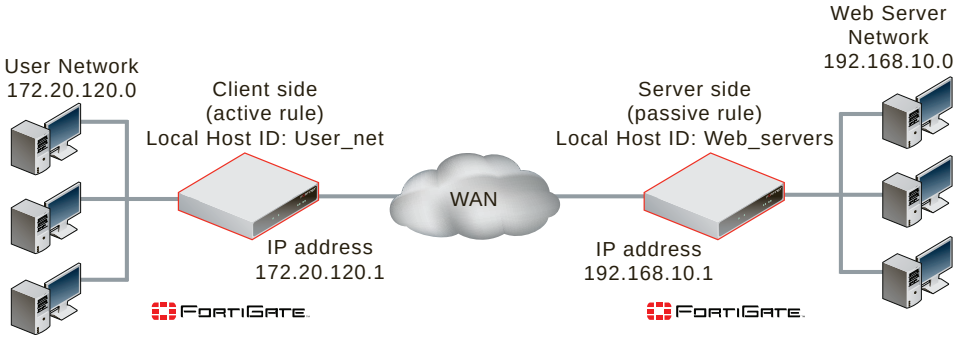
Its also useful to set tunnel-sharing to express-sharing for applications, such as Telnet, that are very interactive but not aggressive. Express sharing optimizes tunnel sharing for interactive applications such as Telnet where latency or delays would seriously affect the user's experience with the protocol.

Set tunnel-sharing to sharing for applications that are not aggressive and are not sensitive to latency or delays. WAN optimization rules set to sharing and express-sharing can share the same tunnel.

Example client/server (active-passive) configuration

The following example shows how to client/server (active-passive) WAN optimization rules for the topology shown in Figure 8. In this example, clients on the user network connect to web servers on the web server network using HTTP on TCP port 80. The FortiGate units are configured to optimize HTTP traffic over the WAN using HTTP protocol optimization, web caching, and byte caching.

Figure 8: Example client/server (active-passive) WAN optimization topology



Client side FortiGate configuration

1 Add the Local Host ID to the client side FortiGate configuration.

```
config wanopt settings
  set host-id User_net
end
```

2 Add the server side Local Host ID to the client side peer list.

```
config wanopt peer
  edit Web_servers
  set ip 192.168.10.1
end
```

3 Add the following active rule to the client side FortiGate unit:

```
config wanopt rule
  edit 2
    set auto-detect active
    set src-ip 172.20.120.0
    set dst-ip 192.168.10.0
    set port 80
  end
```

Accept default settings for `transparent` (`enable`), `proto` (`http`), `status` (`enable`), `mode` (`full`), `byte-caching` (`enable`), `ssl` (`disable`), `secure-tunnel` (`disable`), `auth-group` (`null`), `unknown-http-version` (`tunnel`), and `tunnel-non-http` (`disable`).

Server side FortiGate configuration

1 Add the Local Host ID to the server side FortiGate configuration.

```
config wanopt settings
  set host-id Web_servers
end
```

2 Add the client side Local Host ID to the server side peer list.

```
config wanopt peer
  edit User_net
  set ip 172.20.120.1
```

```
end
```

3 Add the following passive rule to the server side FortiGate unit:

```
config wanopt rule
  edit 5
    set auto-detect passive
    set src-ip 172.20.120.0
    set dst-ip 192.168.10.0
    set port 80
    set webcache enable
  end
```

Accept default settings for `status` (`enable`) and `mode` (`full`).

History

FortiOS v4.0 New.

Related commands

- wanopt auth-group
- wanopt cache-storage
- wanopt peer
- wanopt settings
- wanopt ssl-server
- wanopt storage
- wanopt webcache

settings

Use this command to add or change the FortiGate WAN optimization local host ID and to enable traffic loging for WAN optimization and WAN optimization web caching sessions. The local host ID identifies the FortiGate unit to other FortiGate units for WAN optimization. All WAN optimization tunnel startup requests to other FortiGate units include the local host id. The FortiGate unit can only perform WAN optimization with other FortiGate units that have this local host id in their peer list.

Syntax

```
config wanopt settings
  set host-id <host-id-name_str>
  set log-traffic {cifs ftp http mapi tcp}
end
```

Variable	Description	Default
`host-id <host-id-name_str>`	Enter the local host ID.	default-id
`log-traffic {cifs ftp http mapi tcp}`	Enable WAN optimization and WAN optimization web caching traffic logging for each type of WAN optimization session. Valid types are: `cifs ftp http mapi tcp`. Separate each type with a space. To add or remove an option from the list, retype the complete list as required.	

Example

This example shows how to set the local host ID to `HQ_Peer` and enable traffic logging for WAN optimization CIFS and HTTP sessions.

```
config wanopt settings
  set host-id HQ_peer
  set log-traffic cifs http
end
```

History

FortiOS v4.0 New.

FortiOS 4.0 MR1 Added the `log-traffic` field.

Related commands

- wanopt auth-group
- wanopt cache-storage
- wanopt peer
- wanopt rule
- wanopt ssl-server
- wanopt storage
- wanopt webcache

ssl-server

Use this command to add one or more SSL servers to support WAN optimization SSL offloading. You enable WAN optimization SSL offloading by enabling the `ssl` field in a WAN optimization rule. WAN optimization supports SSL encryption/decryption offloading for HTTP servers.

SSL offloading uses the FortiGate unit to encrypt and decrypt SSL sessions.The FortiGate unit intercepts HTTPS traffic from clients and decrypts it before sending it as clear text to the HTTP server. The clear text response from the HTTP server is encrypted by the FortiGate unit and returned to the client. The result should be a performance improvement because SSL encryption is offloaded from the server to the FortiGate unit FortiASIC SSL encryption/decryption engine.

You must add one WAN optimization SSL server configuration to the FortiGate unit for each HTTP server that you are configuring SSL offloading for. This SSL server configuration must also include the HTTP server CA. You load this certificated into the FortiGate unit as a local certificate using the `config vpn certification local` command and then add the certificate to the SSL server configuration using the `ssl-cert` field. The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

You can configure one WAN optimization rule to offload SSL encryption/decryption for multiple HTTP servers. To do this, the WAN optimization rule source and destination addresses must be configured so that the rule accepts packets destined for all of the HTTP servers that you want offloading for. Then you must add one SSL server configuration for each of the HTTP servers.

Syntax

```
config wanopt ssl-server
  edit <ssl-server-name>
    set ip <ssl_server_ip_ipv4>
    set port <port_int>
    set ssl-mode {full | half}
    set ssl-cert <certificate_name>
    set ssl-dh-bits {1024 | 1536 | 2048 | 768}
    set ssl-min-version {ssl-3.0 | tls-1.0}
    set ssl-max-version {ssl-3.0 | tls-1.0}
    set ssl-send-empty-frags {disable | enable}
  end
```

Variable	Description	Default
`edit <ssl-server-name>`	Enter a name for the SSL server. It can be any name and this name is not used by other FortiGate configurations.	
`ip <ssl_server_ip_ipv4>`	Enter an IP address for the SSL server. This IP address should be the same as the IP address of the HTTP server that this SSL server will be offloading for. When a session is accepted by a WAN optimization rule with SSL offloading enabled, the destination IP address of the session is matched with this IP address to select the SSL server configuration to use.	0.0.0.0
`port <port_int>`	Enter a port number to be used by the SSL server. Usually this would be port 443 for an HTTPS server. When a session is accepted by a WAN optimization rule with SSL offloading enabled, the destination port of the session is matched with this port to select the SSL server configuration to use.	0
`ssl-mode {full | half}`	Configure the SSL server to operate in `full` mode or `half` mode. Half mode offloads SSL from the backend server to the server-side FortiGate unit.	full

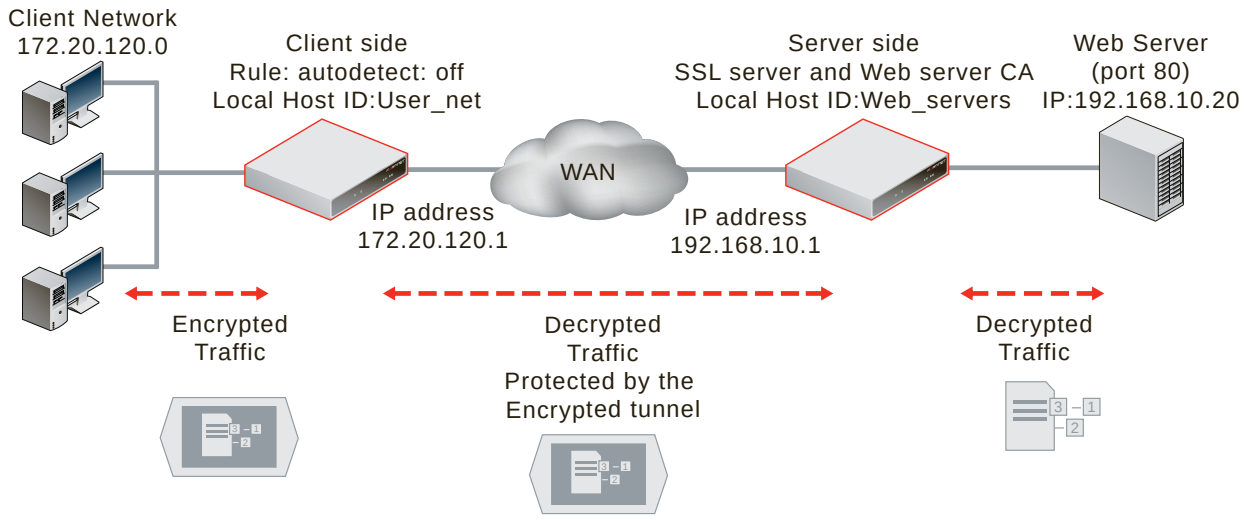
Variable	Description	Default
`ssl-cert <certificate_name>`	Select the certificate to be used for this SSL server. The certificate should be the HTTP server CA used by the HTTP server that this SSL server configuration will be offloading for. The certificate must be a local certificate added to the FortiGate unit using the `config vpn certificate local` command. For more information, see "vpn certificate local" on page 574. The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.	
`ssl-dh-bits {1024 | 1536 | 2048 | 768}`	Select the size of the Diffie-Hellman prime used in DHE_RSA negotiation. Larger primes may cause a performance reduction but are more secure.	`1024`
`ssl-min-version {ssl-3.0 | tls-1.0}`	Select the lowest or oldest SSL/TLS version to offer when negotiating. You can set the minimum version to SSL 3.0 or TLS 1.0. TLS 1.0 is more secure that SSL 3.0.	`ssl-3.0`
`ssl-max-version {ssl-3.0 | tls-1.0}`	Select the highest or newest SSL/TLS version to offer when negotiating. You can set the maximum version to SSL 3.0 or TLS 1.0. TLS 1.0 is more secure that SSL 3.0.	tls-1.0
`ssl-send-empty-frags {disable | enable}`	Enable or disable sending empty fragments before sending the actual payload. Sending empty fragments is a technique used to avoid cipher-block chaining (CBC) plaintext attacks if the initiation vector (IV) is known. Also called the CBC IV. Some SSL implementations are not compatible with sending empty fragments. Change `ssl-send-empty-frags` to `disable` if required by your SSL implementation.	enable

Example: SSL offloading for a WAN optimization tunnel

In this example, clients on the user network use https://192.168.10.20 to browse to an HTTP web server. A WAN optimization rule with `auto-detect` set to `off` on the client side FortiGate unit accepts sessions from the clients with source addresses on the 172.20.120.0 network and with a destination address of 192.168.10.0 and with a destination port of 443. In this rule `secure-tunnel` is enabled so that the tunnel is encrypted.

The server side FortiGate unit includes an SSL server configuration with `ip` set to 192.168.10.20 and `port` to 443. The server side FortiGate unit also includes the HTTP server CA.

Figure 9: SSL offloading for byte caching



When the client side FortiGate unit accepts an HTTPS connection for 192.168.10.20 the SSL server configuration provides the information that the client side FortiGate unit needs to decrypt the traffic and send it in clear text across a WAN optimization tunnel to the server side FortiGate unit. The server side FortiGate unit then forwards the clear text packets to the HTTP server.

The HTTP server CA is not downloaded from the server side to the client side FortiGate unit. Instead the client side FortiGate unit proxies the SSL parameters from the client side to the server side which returns an SSL key and other required information to the client side FortiGate unit so that the client FortiGate unit can decrypt and encrypt HTTPS traffic.

Note: You do not need to add a WAN optimization rule to the server side FortiGate unit as long as the server side FortiGate unit includes the local host ID of the client FortiGate unit in its peer list. However, you could set `auto-detect` to `active` on the client side FortiGate and add then a rule to the server side FortiGate unit with `auto-detect` set to `passive`.

Note: In this example the secure tunnel and the authentication group configurations are not required, but are added to enhance security. Adding the peers and the WAN optimization rules are required for WAN optimization SSL offloading.

To configure the client side FortiGate unit

1 Enter the following command to set the local host ID of the client side FortiGate unit to `User_net`.

```
config wanopt settings
  set host-id User_net
end
```

2 Enter the following command to add the server side local host ID to the client side FortiGate unit.

```
config wanopt peer
  edit Web_servers
    set ip 192.168.10.1
  end
```

3 Enter the following command to add an authentication group named `SSL_auth_grp` to the client side FortiGate unit. The authentication group includes a preshared key and the peer added in step 2. An authentication group with the same name and the same preshared key must also be added to the server side FortiGate unit. This authentication group is required for the secure tunnel.

```
config wanopt auth-grp
  edit SSL_auth_grp
    set auth-method psk
    set psk <preshared_key>
    set peer-accept one
    set peer Web_servers
  end
```

4 Enter the following command to add the WAN optimization rule:

```
config wanopt rule
  edit 5
    set src-ip 172.20.120.0
    set dst-ip 192.168.10.0
    set port 443
    set peer Web_servers
    set ssl enable
    set secure-tunnel enable
    set auth-group SSL_auth_grp
    set webcache enable
  end
```

You can configure other rule settings as required. By default `transparent` is enabled, `proto` is `http` (`proto` should not be changed), `mode` is `full`, `auto-detect` is `off`, `byte-caching` is enabled, and `tunnel-sharing` is `private`.

To configure the server side FortiGate unit

1 Enter the following command to set the local host ID of the server side FortiGate unit to `Web_servers`.

```
config wanopt settings
  set host-id Web_servers
end
```

2 Enter the following command to add the client side local host ID to the server side FortiGate unit.

```
config wanopt peer
  edit User_net
    set ip 172.20.120.1
  end
```

3 Enter the following command to add an authentication group named `SSL_auth_grp` to the server side FortiGate unit. The authentication group includes a preshared key and the peer added to the server side FortiGate unit in step 2.

```
config wanopt auth-grp
  edit SSL_auth_grp
    set auth-method psk
    set psk <preshared_key>
    set peer-accept one
    set peer User_net
  end
```

4 Use the `config vpn certificate local` command to add the HTTP server CA. Set the name of the local certificate to `Web_Server_Cert_1`.

The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

5 Enter the following command to add the SSL server to the server side FortiGate unit.

```
config wanopt ssl-server
  edit example_server
    set ip 192.168.10.20
    set port 443
    set ssl-cert Web_Server_Cert_1
  end
```

Configure other `ssl-server` settings as required for your configuration.

History

FortiOS v4.0 New.

Related commands

- wanopt auth-group
- wanopt cache-storage
- wanopt peer
- wanopt rule
- wanopt settings
- wanopt storage, wanopt webcache

storage

Use the `show wanopt storage` command to view WAN optimization storages. Use the `config wanopt storage` command to change the size of WAN optimization storages. A storage defines the maximum size of the byte caching or web caching database added to the storage.

You use the `execute scsi-dev storage` command to add WAN optimization storages. For more information about the `execute scsi-dev` command, see "execute scsi-dev" on page 735.

Syntax

```
config wanopt storage
  edit <storage_name_str>
    set partition-label <partition-label>
    set partition-size <partition_size_int>
    set storage-size <storage_size_int>
  end
```

Variable	Description	Default
`edit <storage_name_str>`	Enter the name of the storage added using the `execute scsi-dev storage` command.	
`partition-label <partition-label>`	The random string used to label the partition. You cannot change the partition label.	
`partition-size <partition_size_int>`	The size of the partition in Mbytes. You cannot change the partition size.	
`storage-size <storage_size_int>`	The size of the storage in Mbytes. You can use this field to change the storage size.	

Examples

Use the following command to display all of the storages added to a FortiGate unit. The two storages shown in the output were added to the same partition.

```
show wanopt storage
config wanopt storage
  edit "storage_1"
    set partition-label "742FD71029DB5130"
    set partition-size 76316
    set storage-size 30000
  next
  edit "storage_2"
    set partition-label "742FD71029DB5130"
    set partition-size 76316
    set storage-size 30000
  next
end
```

Use the following command to change the size of `storage_2` from 30000 to 40000 Mbytes:

```
config wanopt storage
  edit "storage_2"
    set storage-size 40000
  next
end
```

History

FortiOS v4.0 New.

Related commands

- wanopt auth-group
- wanopt cache-storage
- wanopt peer
- wanopt rule
- wanopt settings
- wanopt ssl-server
- wanopt webcache

webcache

Use this command to change how the WAN optimization web cache operates. In most cases the default settings are acceptable. However you may want to change these settings to improve performance or optimize the cache for your configuration.

Syntax

```
config wanopt storage
  set always-revalidate {disable | enable}
  set cache-expired {disable | enable}
  set default-ttl <expiry_time>
  set explicit {disable | enable}
  set fresh-factor <fresh_percent>
  set ignore-conditional {disable | enable}
  set ignore-ie-reload {disable | enable}
  set ignore-ims {disable | enable}
  set ignore-pnc {disable | enable}
  set max-object-size <object_size>
  set max-ttl <expiry_time>
  set min-ttl <expiry_time>
  set neg-resp-time <response_time>
  set reval-pnc {disable | enable}
end
```

Variable	Description	Default
`always-revalidate {disable | enable}`	Enable to always to revalidate the requested cached object with content on the server before serving it to the client.	enable
`cache-expired {disable | enable}`	Applies only to type-1 objects. When this setting is enabled, type-1 objects that are already expired at the time of acquisition are cached (if all other conditions make the object cachable). When this setting is disabled, already expired type-1 objects become non-cachable at the time of acquisition.	disable
`default-ttl <expiry_time>`	The default expiry time for objects that do not have an expiry time set by the web server. The default expiry time is 1440 minutes (24 hours).	`1440`
`explicit {disable | enable}`	Enable or disable using the WAN optimization web cache to cache for the explicit proxy.	enable
`fresh-factor <fresh_percent>`	Set the fresh factor as a percentage. The default is 100, and the range is 1 to 100. For cached objects that don't have an expiry time, the web cache periodically checks the server to see if the object has expired. The higher the fresh factor the less often the checks occur.	`100`
`ignore-conditional {disable | enable}`	Enable or disable controlling the behavior of cache-control header values. HTTP 1.1 provides additional controls to the client over the behavior of caches concerning the staleness of the object. Depending on various Cache-Control headers, the FortiGate unit can be forced to consult the OCS before serving the object from the cache. For more information about the behavior of cache-control header values, see RFC 2616.	disable
`ignore-ie-reload {disable | enable}`	Some versions of Internet Explorer issue Accept / header instead of Pragma nocache header when you select Refresh. When an Accept header has only the / value, the FortiGate unit treats it as a PNC header if it is a type-N object. When this option is enabled, the FortiGate unit ignores the PNC interpretation of the Accept: / header.	enable

Variable	Description	Default
`ignore-ims {disable | enable}`	Be default, the time specified by the if-modified-since (IMS) header in the client's conditional request is greater than the last modified time of the object in the cache, it is a strong indication that the copy in the cache is stale. If so, HTTP does a conditional GET to the Overlay Caching Scheme (OCS), based on the last modified time of the cached object. Enable `ignore-ims` to override this behavior.	disable
`ignore-pnc {disable | enable}`	Typically, if a client sends an HTTP GET request with a pragma no-cache (PNC) or cache-control nocache header, a cache must consult the OCS before serving the content. This means that the FortiGate unit always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh. Because of this, PNC requests can degrade performance and increase server-side bandwidth utilization. However, if `ignore-pmc` is enabled, then the PNC header from the client request is ignored. The FortiGate unit treats the request as if the PNC header is not present at all.	disable
`max-object-size <object_size>`	Set the maximum object size to cache. The default size is 512000 kbytes (512 Mbytes). This object size determines the maximum object size to store in the web cache. All objects retrieved that are larger than the maximum size are delivered to the client but are not stored in the web cache.	512000
`max-ttl <expiry_time>`	The maximum amount of time an object can stay in the web cache without checking to see if it has expired on the server. The default is 7200 minutes (120 hours or 5 days).	`7200`
`min-ttl <expiry_time>`	The minimum amount of time an object can stay in the web cache before checking to see if it has expired on the server. The default is 5 minutes.	5
`neg-resp-time <response_time>`	Set how long in minutes to cache negative responses. The default is 0, meaning negative responses are not cached. The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web cache is configured to cache these negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes.	0
`reval-pnc {disable | enable}`	The pragma-no-cache (PNC) header in a client's request can affect the efficiency of the FortiGate unit from a bandwidth gain perspective. If you do not want to completely ignore PNC in client requests (which you can do by using the ignore PNC option configuration), you can lower the impact of the PNC by enabling `reval-pnc`. When the `reval-pnc` is enabled, a client's non-conditional PNC-GET request results in a conditional GET request sent to the OCS if the object is already in the cache. This gives the OCS a chance to return the 304 Not Modified response, consuming less server-side bandwidth, because it has not been forced to return full content even though the contents have not actually changed. By default, the revalidate PNC configuration is disabled and is not affected by changes in the top-level profile. When the Substitute Get for PNC configuration is enabled, the revalidate PNC configuration has no effect. Most download managers make byte-range requests with a PNC header. To serve such requests from the cache, the `reval-pnc` option should be enabled along with byte-range support.	disable

History

FortiOS v4.0 New.

Related commands

- wanopt auth-group, wanopt cache-storage
- wanopt peer, wanopt rule
- wanopt settings, wanopt ssl-server, wanopt storage

web-proxy

Use these commands to configure the FortiGate web proxy. You can use the FortiGate web proxy and interface settings to enable explicit HTTP and HTTPS proxying on one or more interfaces. When enabled, the FortiGate unit becomes a web proxy server. All HTTP and HTTPS session received by interfaces with explicit web proxy enabled are intercepted by the explicit web proxy relayed to their destinations.

To use the explicit proxy, users must add the IP address of a FortiGate interface and the explicit proxy port number to the proxy configuration settings of their web browsers.

On FortiGate units that support WAN optimization, you can also enable web caching for the explicit proxy.

explicit

Use this command to enable the explicit web proxy, and configure the TCP port used by the explicit proxy..

Syntax

```
config web-proxy explicit
  set http-incoming-port <port_num>
  set status {enable | disable}
  set unknown-http-version {best-effort | reject}
end
```

Variable	Description	Default
`http-incoming-port <port_num>`	Select the port the incoming HTTP traffic will use. Valid numbers range from 0 to 65535. The default value of `0` means port 8080.	0
`status {enable | disable}`	Enable the explicit web proxy.	disable
`unknown-http-version {best-effort | reject}`	Select the action to take when an unknown version of HTTP is encountered. Best effort attempts to handle the HTTP traffic as best as it can. Reject treats the HTTP traffic as malformed.	reject

Example

Use the following command to enable the explicit web proxy on the FortiGate `port1` interface so that users can use this interface and its IP address as an explicit proxy server for their web browsers.

```
config system interface
  edit port1
    set explicit-web-proxy enable
end
```

Use the following command to enable the explicit proxy and set the TCP port that proxy accepts connections on to 8080. The result of this configuration is that TCP sessions received by the FortiGate unit at port1 with a destination port number of 8888 are processed by the explicit web proxy.

```
config web-proxy explicit
  set status enable
  set http-incoming-port 8888
end
```

Use the following command to enable web caching for the explicit web proxy on FortiGate units that support WAN optimization and web caching.

```
config wanopt webcache
  set explicit enable
end
```

History

FortiOS v4.0 New.

Related commands

- web-proxy global

global

Configure global web-proxy settings that control how the web proxy functions and handles web traffic. In most cases you should not have to change the default settings of this command. If your FortiGate unit is operating with multiple VDOMS these settings affect all VDOMs.

Syntax

```
config web-proxy global
  set add-header-client-ip {disable | enable}
  set add-header-front-end-https {disable | enable}
  set add-header-via {disable | enable}
  set add-header-x-forwarded-for {disable | enable}
  set forward-proxy-auth {disable | enable}
  set max-message-length <kBytes>
  set max-request-length <kBytes>
  set proxy-fqdn <fqdn>
  set strict-web-check {disable | enable}
end
```

Variable	Description	Default
`add-header-client-ip {disable | enable}`	Enable to add the client IP to the header of forwarded requests	`disable`
`add-header-front-end-https {disable | enable}`	Enable to add a front-end-https header to forwarded requests.	`disable`
`add-header-via {disable | enable}`	Enable to add the via header to forwarded requests.	`disable`
`add-header-x-forwarded-for {disable | enable}`	Enable to add x-forwarded-for header to forwarded requests.	`disable`
`forward-proxy-auth {disable | enable}`	In explicit mode, enable to forward proxy authentication headers. By default proxy authentication headers are blocked by the explicit web proxy. You can set this option to enable if you need to allow proxy authentication through the explicit web proxy. This option does not apply to web proxy transparent mode, because in transparent mode, proxy authentication headers are always forwarded by the web proxy.	`disable`
`max-message-length <kBytes>`	Set the maximum length, in kBytes, of the HTTP message not including body. Range 16 to 256.	32
`max-request-length <kBytes>`	Set the maximum length, in kBytes, of the HTTP request line. Range 2 to 64.	4
`proxy-fqdn <fqdn>`	Set the fully qualified domain name (FQDN) for the proxy. This is the domain that clients connect to.	`default.fqdn`
`strict-web-check {disable | enable}`	Enable to block web sites that send incorrect headers that do not conform to HTTP 1.1 as described in RFC 2616. Disable to allow and cache website that send incorrect headers that do not conform to the RFC. This option is disabled by default so that web sites are not blocked. You can enable this option if you want to increase security by blocking sites that do not conform. Enabling this option may block some commonly used websites.	`disable`

Example

Use the following command to configure the explicit proxy to block web sites that send incorrect headers that do not conform with HTTP 1.1

```
config web-proxy global
  set strict-web-check enable
end
```

History

FortiOS v4.0	New.
FortiOS v4.1	Added the options `forward-proxy-auth` and `strict-web-check`.

Related commands

- web-proxy explicit

webfilter

Use webfilter commands to add banned words to the banned word list, filter URLs, and configure FortiGuard-Web category filtering.

For more information about web filtering see the *FortiGate UTM User Guide*.

This chapter contains the following sections:

content

Control web content by blocking or exempting words, phrases, or patterns. If enabled in the protection profile, the FortiGate unit searches for words or patterns on requested web pages.

For each pattern you can select *Block* or *Exempt*. Block, blocks access to a web page that matches with the pattern. Exempt allows access to the web page even if other entries in the list that would block access to the page.

For a page, each time a block match is found values assigned to the pattern are totalled. If a user-defined threshold value is exceeded, the web page is blocked.

Use this command to add or edit and configure options for the Web content filter list. Patterns words can be one word or a text string up to 80 characters long. The maximum number of patterns in the list is 5000.

When a single word is entered, the FortiGate unit checks Web pages for that word. Add phrases by enclosing the phrase in ‘single quotes’. When a phrase is entered, the FortiGate unit checks Web pages for any word in the phrase. Add exact phrases by enclosing the phrases in “quotation marks”. If the phrase is enclosed in quotation marks, the FortiGate checks Web pages for the exact phrase.

Create patterns using wildcards or Perl regular expressions. See “Using Perl regular expressions” on page 50.

You can add multiple web content filter lists, and then select the list for each protection profile.

Note: Perl regular expression patterns are case sensitive for Web Content Filtering. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` blocks all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

Syntax

```
config webfilter content
  edit <entry_number>
    set name <list_str>
    set comment <comment_str>
    config entries
      edit <content_str>
        set action {block | exempt}
        set lang {french | japanese | korean | simch | spanish |thai | trach
           | western}
        set pattern-type {regexp | wildcard}
        set score <score_int>
        set status {enable | disable}
      end
  end
```

Variable	Description	Default
`edit <entry_number>`	A unique number to identify the banned word list.	
`name <list_str>`	The name of the banned word list.	
`comment <comment_str>`	The comment attached to the banned word list.	
`config entries` Variables		
`edit <content_str>`	Enter the content to match.	

Variable	Description	Default
`action {block | exempt}`	Select one of: `block` If the pattern matches, the Score is added to the total for the web page. The page is blocked if the total score of the web page exceeds the web content block threshold defined in the protection profile. `Exempt` If the pattern matches, the web page will not be blocked even if there are matching Block entries.	`block`
`lang {french | japanese | korean | simch | spanish |thai | trach | western}`	Enter the language character set used for the content. Choose from French, Japanese, Korean, Simplified Chinese, Spanish, Thai, Traditional Chinese, or Western.	`western`
`pattern-type {regexp | wildcard}`	Set the pattern type for the content. Choose from `regexp` or `wildcard`.Create patterns for banned words using Perl regular expressions or wildcards.	`wildcard`
`score <score_int>`	A numerical weighting applied to the content. The score values of all the matching words appearing on a web page are added, and if the total is greater than the `webwordthreshold` value set in the protection profile, the page is processed according to whether the `bannedword` option is set with the `http` command in the protection profile. The score for banned content is counted once even if it appears multiple times on the web page.	10
`status {enable | disable}`	Enable or disable the content entry.	`disable`

History

FortiOS 4.0 MR1 New, Replaces `config webfilter block` and `config webfilter exmword`.

Related topics

- webfilter fortiguard
- webfilter ftgd-local-cat
- webfilter ftgd-local-rating
- webfilter ftgd-ovrd
- webfilter ftgd-ovrd-user
- webfilter urlfilter

content-header

Use this example to filter web content according to the MIME content header. You can use this feature to broadly block content by type. But it is also useful to exempt audio and video streaming files from antivirus scanning. Scanning these file types can be problematic.

The content header list is available in the CLI only.

Syntax

```
config webfilter content-header
  edit <entry_number>
    set name <list_name>
    set comment <comment_str>
    config entries
      edit <regex>
        set action {block | exempt}
      end
  end
```

c

Variable	Description	Default
`edit <entry_number>`	A unique number to identify the content header list.	
`name <list_name>`	The name of the content header list.	
`comment <comment_str>`	The comment attached to the content header list.	
`config entries` Variables		
`edit <regex>`	Enter a regular expression to match the content header. For example, `.*image.*` matches image content types.	
`action {block | exempt}`	Select one of: `block` If the pattern matches, the content is blocked. `exempt` If the pattern matches, the content is exempted from antivirus scanning.	`block`

After you have created content header lists, you need to select the content header list in the protection profile as follows:

```
config firewall profile
  edit <profile_name>
    ...
    set content-header-list <list_name>
    ...
  end
```

History

FortiOS 4.0 MR1 New.

Related topics

- webfilter fortiguard, webfilter ftgd-local-cat, webfilter ftgd-local-rating
- webfilter ftgd-ovrd, webfilter ftgd-ovrd-user
- webfilter urlfilter

fortiguard

Use this command to enable Web filtering by specific categories using FortiGuard-Web URL filtering.

FortiGuard-Web category blocking

FortiGuard-Web is a web filtering solution provided by Fortinet. FortiGuard-Web sorts thousands of Web pages into a wide variety of categories that users can allow, block, or monitor. Categories are also organized into broader groups to make configuration fast and easy. The FortiGate unit accesses the nearest FortiGuard-Web server to determine the category of a requested web page and then follows the firewall policy configured for that user or interface. FortiGuard-Web servers are located worldwide.

FortiGuard-Web licensing

Every FortiGate unit comes with a free 30 day FortiGuard-Web trial license. FortiGuard-Web license management is done by the FortiGuard-Web server, so there is no need to enter a license number. The FortiGate unit automatically contacts the FortiGuard-Web servers when FortiGuard-Web category blocking is enabled.

To renew the FortiGuard-Web license after the free trial, contact Fortinet Technical Support.

FortiGuard-Web configuration

Once enabled, FortiGuard-Web category block settings apply globally. After enabling FortiGuard-Web, configure different categories for each firewall protection profile create.

See “firewall profile” on page 139 to configure FortiGuard-Web category blocking in a protection profile.

See “FortiGuard-Web categories” in the *FortiGate Administration Guide* for a complete list and description of the FortiGuard-Web web filter categories.

HTTP and HTTPS FortiGuard override traffic

The FortiGuard override for HTTP and HTTPS is no longer a single global forward rule. Instead, a separate rule is created for each protection profile to redirect both the FortiGuard override HTTP and HTTPS ports, as required, into the authentication daemon. This ensures that these ports only appear open when the appropriate options are enabled in the profile. A matrix of how the profile options affect the port status follows:

HTTP WF	HTTP ovrd	HTTPS WF	ovrd via HTTPS	HTTP Port	HTTPS Port
0	0	0	0	closed	closed
0	0	0	1	closed	closed
0	0	1	0	closed	open
0	0	1	1	closed	open
0	1	0	0	closed	closed
0	1	0	1	closed	closed
0	1	1	0	closed	open
0	1	1	1	closed	open
1	0	0	0	open	closed
1	0	0	1	open	closed
1	0	1	0	open	open
1	0	1	1	open	open
1	1	0	0	open	closed
1	1	0	1	open	open

1	1	1	0	open	open
1	1	1	1	open	open

There are two separate ports for HTTP and HTTPS override traffic which can be configured independently.

In addition, HTTPS uses the HTTPS override form regardless of the `ovrd-auth-https` status. If `ovrd-auth-https` is enabled, any attempts to use the HTTP version of the override form will transparently be re-directed to the HTTPS version.

Syntax

```
config webfilter fortiguard
  set cache-mode {ttl | db-ver}
  set cache-mem-percent <percent_integer>
  set cache-prefix-match <enable | disable>
  set ovrd-auth-port-http <port_integer>
  set ovrd-auth-https <enable | disable>
  set ovrd-auth-port-https <port_integer>
  set reports-status <enable | disable>
end
```

Variable	Description	Default
`cache-mode {ttl | db-ver}`	Change the cache entry expiration mode. Choices are `ttl` or `db-ver`. Using `ttl`, cache entries are deleted after a number of seconds determined by the `cache-ttl` setting, or until newer cache entries force the removal of older ones. When set to `db-ver`, cache entries are kept until the FortiGuard database changes, or until newer cache entries force the removal of older ones.	`ttl`
`cache-mem-percent <percent_integer>`	Change the maximum percentage of memory the cache will use. Enter a value from 1 to 15 percent.	2
`cache-prefix-match <enable | disable>`	Enable and disable prefix matching. If enabled the FortiGate unit attempts to match a packet against the rules in a prefix list starting at the top of the list. For information on prefix lists see the section "prefix-list, prefix-list6" on page 337 of the Router chapter in the FortiOS CLI Guide.	enable
`ovrd-auth-port-http <port_integer>`	The port to use for FortiGuard Web Filter HTTP override authentication.	`8008`
`ovrd-auth-https <enable | disable>`	Enable to use HTTPS for override authentication.	`disable`
`ovrd-auth-port-https <port_integer>`	The port to use for FortiGuard Web filtering HTTPS override authentication.	`8010`
`reports-status <enable | disable>`	Enable or disable FortiGuard Web Filter reports. This feature is available only on FortiGate units with an internal hard disk.	`disable`

History

FortiOS v2.80 New.

FortiOS v2.80 MR2 Added `cerb_hostname`, `cerb_port`, `ftgd_hostname`, and, `ftgd_port` fields. Changed `license` to `cerb_license`.

FortiOS v2.80 MR4	Removed `cerb_hostname`, `cerb_license`, and, `cerb_port` fields. Removed `ftgd_port` field.
FortiOS v3.0	Add `cache-mode`, `cache-mem-percent`, `license`, `expiration`, `hostname`, `img-sink-ip`, `ovrd-auth-port`, `ovrd-auth-https`, and, `port`. Removed `ftgd_hostname`, and, `service`. Name changed from catblock to fortiguard.
FortiOS v3.0 MR1	Many of the commands were moved to “config system fortiguard” and some new commands were added.
FortiOS v3.0 MR3	`cache-prefix-match <enable | disable>` command added.
FortiOS v3.0 MR4	Removed the command `ovrd-auth-port` replaced with `ovrd-auth-port-http`. Added the command `ovrd-auth-port-https`. Added new H3 section on HTTP and HTTPS FortiGuard override traffic.
FortiOS v3.0 MR4	Removed the command `img-sink-ip`.
FortiOS v4.0 MR1	Added `reports-status`.

Related topics

- webfilter content
- webfilter ftgd-local-cat
- webfilter ftgd-local-rating
- webfilter ftgd-ovrd
- webfilter ftgd-ovrd-user
- webfilter urlfilter

ftgd-local-cat

Use this command to add local categories to the global URL category list. The categories defined here appear in the global URL category list when configuring a protection profile. Users can rate URLs based on the local categories.

Syntax

```
config webfilter ftgd-local-cat
  edit <local_cat_str>
    set id <id_int>
  end
```

Variable	Description	Default
<local_cat_str>	The description of the local category.	
id <id_int>	The local category unique ID number.	140

Example

This example shows how to add the category local_block with an ID of 155.

```
config webfilter ftgd-local-cat
  edit local_block
    set id 155
  end
```

History

FortiOS v3.0 New

Related topics

- webfilter content
- webfilter fortiguard
- webfilter ftgd-local-rating
- webfilter ftgd-ovrd
- webfilter ftgd-ovrd-user
- webfilter urlfilter

ftgd-local-rating

Use this command to rate URLs using local categories.

Users can create user-defined categories then specify the URLs that belong to the category. This allows users to block groups of web sites on a per profile basis. The ratings are included in the global URL list with associated categories and compared in the same way the URL block list is processed.

The user can also specify whether the local rating is used in conjunction with the FortiGuard rating or is used as an override.

Syntax

```
config webfilter ftgd-local-rating
  edit <url_str>
    set rating [[<category_int>] [group_str] [class_str]...]
    set status {enable | disable}
  end
```

Variable	Description	Default
`<url_str>`	The URL being rated.	
`rating [[<category_int>] [group_str] [class_str]...]`	Set categories, groups, and classifications for the rating. Enter '?' to print a list of category codes and descriptions available. To remove categories from the rating, use the unset command.	
`status {enable | disable}`	Enable or disable the local rating.	`enable`

Example

This example shows how to configure a local rating for the web site www.example.com. with a rating including category 12, all categories in group 4, and classification 1.

```
config webfilter ftgd-local-rating
  edit www.example.com
    set rating 12 g4 c1
  end
```

History

FortiOS v3.0 New

Related topics

- webfilter content
- webfilter fortiguard
- webfilter ftgd-local-cat
- webfilter ftgd-ovrd
- webfilter ftgd-ovrd-user
- webfilter urlfilter

ftgd-ovrd

Use this command to configure FortiGuard-Web filter administrative overrides.

The administrative overrides are backed up with the main configuration and managed by the FortiManager system. The administrative overrides are not cleaned up when they expire and you can reuse these override entries by extending their expiry dates.

Users may require access to web sites that are blocked by a policy. In this case, an administrator can give the user the ability to override the block for a specified period of time.

When a user attempts to access a blocked site, if override is enabled, a link appears on the block page directing the user to an authentication form. The user must provide a correct user name and password or the web site remains blocked. Authentication is based on user groups and can be performed for local, RADIUS, and LDAP users.

Syntax

```
config webfilter ftgd-ovrd
  edit <override_int>
    set expires <yyyy/mm/dd hh:mm:ss>
    set ext-ref <allow | deny>
    set initiator
    set ip <ipv4>
    set ip6 <ipv6>
    set profile <profile_str>
    set rating [[<category_int>] [group_str] [class_str]...]
    set scope {user | user-group | ip | ip6 | profile}
    set status {enable | disable}
    set type {dir | domain | rating}
    set url <url_str>
    set user <user_str>
    set user-group <user_group_str>
  end
get webfilter ftgd-ovrd <override_int>
```

Variable	Description	Default
<override_int>	The unique ID number of the override.	
expires <yyyy/mm/dd hh:mm:ss>	The date and time the override expires. For example, the command to configure an expiry time of 6:45 p.m. on May 22, 2009 would be formatted this way: set expires 2010/05/22 18:45:00	15 minutes after the override is created.
ext-ref <allow | deny>	Allow or deny access to off-site URLs.	allow
initiator	The user who initiated the override rule. This field is get-only.	
ip <ipv4>	When the scope is ip, enter the IP address for which the override rule applies.	0.0.0.0
ip6 <ipv6>	When the scope is ip6, enter the IP address for which the override rule applies.	::
profile <profile_str>	When the scope is profile, enter the profile for which the override rule applies.	
rating [[<category_int>] [group_str] [class_str]...]	If type is set to rating, set the categories, groups, and classifications to override. Enter ? to print a list of category codes and descriptions available. To remove categories from the rating, use the unset command.	

Variable	Description	Default
`scope {user | user-group | ip | ip6 | profile}`	The scope of the override rule.	user
`status {enable | disable}`	Enable or disable the override rule.	disable
`type {dir | domain | rating}`	Specify the type of override rule. • dir - override the website directory • domain - override the domain • rating - override the specified categories and classifications	`dir`
`url <url_str>`	The URL for which the override rule applies.	
`user <user_str>`	When the scope is `user`, the user for which the override rule applies.	
`user-group <user_group_str>`	When the scope is user group, enter the user group for which the override rule applies.	

Example

This example shows how to set an override (13).

```
config webfilter ftgd-ovrd
  edit 13
    set rating 12 g4 c1
  end
```

Use the following command to get information about an override.

```
#get webfilter ftgd-ovrd 1

id                  : 1
expires             : Wed Jul  6 07:00:30 2009
ext_ref             : allow
initiator           : admin
scope               : user
status              : enable
type                : dir
url                 : 192.168.220.23
user                : user_1
```

History

FortiOS v3.0	New
FortiOS v4.0 MR1	Added `ip6` option to `scope`. Added `ip6` field.

Related topics

- webfilter content
- webfilter fortiguard
- webfilter ftgd-local-cat
- webfilter ftgd-local-rating
- webfilter ftgd-ovrd-user
- webfilter urlfilter

ftgd-ovrd-user

Use this command to configure FortiGuard-Web filter user overrides.

When a user attempts to access a blocked site, if override is enabled, a link appears on the block page directing the user to an authentication form. The user must provide a correct user name and password or the web site remains blocked. Authentication is based on user groups and can be performed for local, RADIUS, and LDAP users.

Administrators can only view and delete the user overrides entries.

Syntax

```
config webfilter ftgd-ovrd-user
  edit <override_int>
    set expires <yyyy/mm/dd hh:mm:ss>
    set ext-ref <allow | deny>
    set initiator
    set ip <ipv4>
    set ip6 <ipv6>
    set profile <profile_str>
    set rating [[<category_int>] [group_str] [class_str]...]
    set scope {user | user-group | ip | profile}
    set status {enable | disable}
    set type {dir | domain | rating}
    set url <url_str>
    set user <user_str>
    set user-group <user_group_str>
  end
get webfilter ftgd-ovrd-user <override_int>
```

Variable	Description	Default
<override_int>	The unique ID number of the override.	
expires <yyyy/mm/dd hh:mm:ss>	The date and time the override expires. For example, the command to configure an expiry time of 6:45 p.m. on May 22, 2009 would be formatted this way: set expires 2010/05/22 18:45:00	15 minutes after the override is created.
ext-ref <allow | deny>	Allow or deny access to off-site URLs.	allow
initiator	The user who initiated the override rule. This field is get-only.	
ip <ipv4>	When the scope is IP, enter the IP address for which the override rule applies.	0.0.0.0
ip6 <ipv6>	When the scope is ip6, enter the IP address for which the override rule applies.	::
profile <profile_str>	When the scope is profile, enter the profile for which the override rule applies.	
rating [[<category_int>] [group_str] [class_str]...]	If type is set to rating, set the categories, groups, and classifications to override. Enter ? to print a list of category codes and descriptions available. To remove categories from the rating, use the unset command.	
scope {user | user-group | ip | profile}	The scope of the override rule.	user
status {enable | disable}	Enable or disable the override rule.	disable

Variable	Description	Default
type {dir | domain | rating}	Specify the type od override rule. • dir - override the website directory • domain - override the domain • rating - override the specified categories and classifications	dir
url <url_str>	The URL for which the override rule applies.	
user <user_str>	When the scope is user, the user for which the override rule applies.	
user-group <user_group_str>	When the scope is user group, the user group for which the override rule applies.	

Example

This example shows how to set an override (12).

```
config webfilter ftgd-ovrd-user
  edit 12
    set scope ip
    set ip 192.168.220.23
  end
```

Use the following command to get information about an override.

```
#get webfilter ftgd-ovrd-user 1

id                  : 1
expires             : Wed Jul  6 07:00:30 2005
ext_ref             : allow
initiator           : user
scope               : user
status              : enable
type                : dir
url                 : 192.168.220.23
user                : user_1
```

History

FortiOS v3.0 MR7 New

Related topics

- webfilter content
- webfilter fortiguard
- webfilter ftgd-local-cat
- webfilter ftgd-local-rating
- webfilter ftgd-ovrd
- webfilter urlfilter

urlfilter

Use this command to control access to specific URLs by adding them to the URL filter list. The FortiGate unit exempts or blocks Web pages matching any specified URLs and displays a replacement message instead.

Configure the FortiGate unit to allow, block, or exempt all pages on a website by adding the top-level URL or IP address and setting the action to allow, block, or exempt.

Block individual pages on a website by including the full path and filename of the web page to block. Type a top-level URL or IP address to block access to all pages on a website. For example, `www.example.com` or `172.16.144.155` blocks access to all pages at this website.

Type a top-level URL followed by the path and filename to block access to a single page on a website. For example, `www.example.com/news.html` or `172.16.144.155/news.html` blocks the news page on this website.

To block all pages with a URL that ends with `example.com`, add `example.com` to the block list. For example, adding `example.com` blocks access to `www.example.com`, `mail.example.com`, `www.finance.example.com`, and so on.

Use this command to exempt or block all URLs matching patterns created using text and regular expressions (or wildcard characters). For example, `example.*` matches `example.com`, `example.org`, `example.net` and so on. The FortiGate unit exempts or blocks Web pages that match any configured pattern and displays a replacement message instead.

The maximum number of entries in the list is 5000.

Syntax

```
config webfilter urlfilter
  edit <list_int>
    set name <list_srt>
    set comment <comment_str>
    config entries
      edit <url_str>
        set action {allow | block | exempt}
        set status {enable | disable}
        set type {simple | regex | wildcard}
    end
  end
```

Variable	Description	Default
`<list_int>`	A unique number to identify the URL filter list.	
`<list_srt>`	The name of the URL filter list.	
`<comment_str>`	The comment attached to the URL filter list.	
`<url_str>`	The URL to added to the list.	
`action {allow | block | exempt}`	The action to take for matches. An `allow` match exits the URL filter list and checks the other web filters. An `exempt` match stops all further checking including AV scanning. A `block` match blocks the URL and no further checking will be done.	`exempt`
`status {enable | disable}`	The status of the filter.	`enable`
`type {simple | regex | wildcard}`	The type of URL filter: simple, regular expression, or wildcard.	`simple`

History

FortiOS v3.0	New
FortiOS v3.0 MR4	All models have the same CLI syntax now.
FortiOS v4.0 MR1	Added `wildcard` option to `type`.

Related topics

- webfilter content
- webfilter fortiguard
- webfilter ftgd-local-cat
- webfilter ftgd-local-rating
- webfilter ftgd-ovrd
- webfilter ftgd-ovrd-user

wireless-controller

These commands configure the wireless controller feature. They do not apply to wireless features of FortiWiFi models.

Any FortiGate unit except model 30B or the FortiWiFi models can act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi units. All units must run FortiOS 4.0 MR1.

You create virtual access points that can be associated with multiple physical access points. Clients can roam amongst the physical access points, extending the range of the wireless network.

To use the wireless controller feature, you must enable it as follows:

```
config system global
  set wireless-controller enable
end
```

This chapter describes the following commands:

ap-status

Use this command to designate detected access points as accepted or rogue.

To get information about detected access points, use the `get wireless-controller scan` command.

Syntax

```
config wireless-controller ap-status
  edit <ap_id>
    set bssid <bssid>
    set ssid <ssid>
    set status {accepted | rogue}
  end
```

Variable	Description	Default
`<ap_id>`	Enter a number to identify this access point.	No default.
`bssid <bssid>`	Enter the access point's BSSID. This is the wireless AP's wireless MAC address.	`00:00:00:00:00:00`
`ssid <ssid>`	Enter the wireless service set identifier (SSID) or network name for the wireless interface.	No default.
`status {accepted | rogue}`	Select the desired status for this AP: accepted or rogue.	`rogue`

History

FortiOS v4.0 MR1 New.

Related commands

- get wireless-controller scan

global

Use this command to configure global settings for physical access points, also known as WLAN Termination Points (WTPs) configured using Control And Provisioning of Wireless Access Points (CAPWAP) protocol.

Syntax

```
config wireless-controller global
  set ac-radio-type {802.11a 802.11b 802.11g}
  set discovery-mc-addr <ipv4addr>
  set image-update {disable | join}
  set location <string>
  set max-clients <int>
  set max-retransmit <int>
  set name <string>
  set plain-control-message {enable | disable}
end
```

Variable	Description	Default
`ac-radio-type {802.11a 802.11b 802.11g}`	Enter the wireless bands that the access points must support.	`802.11a 802.11b 802.11g`
`discovery-mc-addr <ipv4addr>`	Enter the IP address for AP discovery.	`224.0.1.140`
`image-update {disable | join}`	Enter join to have AP download image file if it needs a firmware update when it joins the network.	`join`
`location <string>`	Enter the location of your wireless network.	No default.
`max-clients <int>`	Enter the maximum number of clients permitted to connect simultaneously. Enter 0 for no limit.	0
`max-retransmit <int>`	Enter the maximum # of retransmissions for tunnel packet. Range 0 to 64.	3
`name <string>`	Enter a name for your wireless network.	No default.
`plain-control-message {enable | disable}`	Enable unencrypted control message. You should use this only for testing.	`disable`

History

FortiOS v4.0 MR1 New.

timers

Use this command to alter timers for physical access points, also known as WLAN Termination Points (WTPs) configured using Control And Provisioning of Wireless Access Points (CAPWAP) protocol.

Syntax

```
config wireless-controller timers
  set client-idle-timeout <seconds>
  set discovery-interval <seconds>
  set echo-interval <seconds>
end
```

Variable	Description	Default
client-idle-timeout <seconds>	Set the timeout period in seconds for inactive clients.	300
discovery-interval <seconds>	Set the period between discovery requests. Range 2 to 180 seconds.	5
echo-interval <seconds>	Set the interval before WTP sends Echo Request after joining AC. Range 1 to 600 seconds.	30

History

FortiOS v4.0 MR1 New.

vap

Use this command to configure Virtual Access Points.

Syntax

```
config wireless-controller vap
  edit <vap_name>
    set auth {PSK | RADIUS}
    set broadcast-ssid {enable | disable}
    set encrypt {AES | TKIP}
    set fast-roaming {enable | disable}
    set key <key_str>
    set keyindex {1 | 2 | 3 | 4}
    set max-clients <int>
    set radius-server <server_name>
    set security {None  | WEP128 | WEP64  | WPA  | WPA2  | WPA2_AUTO}
    set ssid <string>
    set vdom <vdom_name>
  end
```

To retrieve information about a VAP:

```
config wireless-controller vap
  edit <vap_name>
    get
  end
```

The `client-count` is returned, along with the current configuration settings.

Variable	Description	Default
`auth {PSK | RADIUS}`	Select whether authentication is by preshared key (PSK) or RADIUS server. This is available if `security` is a WPA type.	PSK
`broadcast-ssid {enable | disable}`	Enable broadcast of the SSID. Broadcasting the SSID enables clients to connect to your wireless network without first knowing the SSID. For better security, do not broadcast the SSID.	`enable`
`client-count <int>`	Current number of clients on this VAP. Read-only.	
`encrypt {AES | TKIP}`	Select whether VAP uses AES or TKIP encryption. This is available if `security` is a WPA type.	`TKIP`
`fast-roaming {enable | disable}`	Enabling fast-roaming enables pre-authentication where supported by clients.	`enable`
`key <key_str>`	Enter the encryption key that the clients must use. For WEP64, enter 10 hexadecimal digits. For WEP128, enter 26 hexadecimal digits. This is available when `security` is a WEP type.	No default.
`keyindex {1 | 2 | 3 | 4}`	Many wireless clients can configure up to four WEP keys. Select which key clients must use.with this access point. This is available when `security` is a WEP type.	1
`max-clients <int>`	Enter the maximum number of clients permitted to connect simultaneously. Enter 0 for no limit.	0
`passphrase <hex_str>`	Enter the encryption passphrase of 8 to 63 characters. This is available when `security` is a WPA type and `auth` is PSK.	No default.
`radius-server <server_name>`	Enter the RADIUS server used to authenticate users. This is available when `auth` is `RADIUS`.	No default.

Variable	Description	Default
security {None | WEP128 | WEP64 | WPA | WPA2 | WPA2_AUTO}	Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface. None — has no security. Any wireless user can connect to the wireless network. WEP64 — 64-bit web equivalent privacy (WEP). To use WEP64 you must enter a Key containing 10 hexadecimal digits (0?9 a?f) and inform wireless users of the key. WEP128 — 128-bit WEP. To use WEP128 you must enter a Key containing 26 hexadecimal digits (0-9 a-f) and inform wireless users of the key. WPA — Wi-Fi protected access (WPA) security. To use WPA you must select a data encryption method. You must also enter a pre?shared key containing at least eight characters or select a RADIUS server. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server. WPA2 — WPA with more security features. To use WPA2 you must select a data encryption method and enter a pre-shared key containing at least eight characters or select a RADIUS server. If you select a RADIUS server the wireless clients must have accounts on the RADIUS server. WPA2_AUTO — the same security features as WPA2, but also accepts wireless clients using WPA security.	None
ssid <string>	Enter the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.	No default.
<vap_name>	Enter a name for this Virtual Access Point.	No default.
vdom <vdom_name>	Enter the name of the VDOM to which this VAP belongs.	No default.

History

FortiOS v4.0 MR1 New.

vap-group

Use this command to configure VAP groups.

Syntax

```
config wireless-controller vap-group
  edit <vap_group_name>
    set member {vap1 ... vapn}
  end
```

Variable	Description	Default
`member {vap1 ... vapn}`	Enter the members of this VAP group.	No default.
`<vap_group_name>`	Enter a name for this VAP group.	No default.

History

FortiOS v4.0 MR1 New.

Related commands

- wireless-controller vap

wtp

Use this command to configure physical access points (APs) for management by the wireless controller, also known as an access controller (AC).

Syntax

```
config wireless-controller wtp
  edit <fw_sn>
    set admin <admin_status>
    set ap-scan <scan_mode>
    set band {802.11a | 802.11b  | 802.11g}
    set beacon-interval <integer>
    set channel <chan_int>
    set dtim <int>
    set frag-threshold <int>
    set location <string>
    set geography <Americas | EMEA | Israel | Japan | World>
    set max-clients <int>
    set name <string>
    set power-level <dBm>
    set rts-threshold <int>
    set vaps {vap1 ... vapn>
    config deny-mac-list
      edit <mac_id>
        set mac <mac>
      end
    end
  end
```

To retrieve information about a physical access point:

```
config wireless-controller wtp
  edit <fw_sn>
    get
  end
```

Information such as the current number of clients, is returned, along with the current configuration settings.

Variable	Description	Default
`admin <admin_status>`	Set to one of the following: `discovery` — This is the setting for APs that have discovered this AC and registered themselves. To use such an AP, select `enable`. `disable` — Do not manage this AP. `enable` — Manage this AP.	`enable`
`ap-scan <scan_mode>`	Select one of the following modes for access point scanning: `fgscan` — AP performs scanning only and does not provide service. `bgscan` — AP performs scanning during idle periods while acting as an AP. `disable` — Do not perform scanning. Scanning can reduce performance.	`disable`
`band {802.11a | 802.11b | 802.11g}`	Enter the wireless band to use.	`802.11g`

Variable	Description	Default
`beacon-interval <integer>`	Set the interval between beacon packets. Access Points broadcast beacons or Traffic Indication Messages (TIM) to synchronize wireless networks. In an environment with high interference, decreasing the `beacon-interval` might improve network performance. In a location with few wireless nodes, you can increase this value.	`100`
`channel <chan_int>`	Enter the channel for your wireless network or enter `0` to select a channel automatically. The channels that you can select depend on the `geography` setting.	`5`
`dtim <int>`	Set the interval for Delivery Traffic Indication Message (DTIM). Range is 1 to 255.	`1`
`frag-threshold <int>`	Set the maximum packet size that can be sent without fragmentation. Range is 800 to 2346 bytes.	`2346`
`<fw_sn>`	Enter the serial number of the FortiWiFi unit access point.	No default.
`location <string>`	Optionally, enter the location of this AP.	No default.
`geography <Americas | EMEA | Israel | Japan | World>`	Select the country or region in which this FortiWifi unit will operate.	`World`
`max-clients <int>`	Set the maximum number of wireless clients that can use this AP. Enter `0` for no limit.	`0`
`name <string>`	Enter a name to identify this access point.	No default.
`power-level <dBm>`	Set transmitter power level in dBm. Range 0 to 17.	`17`
`rts-threshold <int>`	Set the packet size for RTS transmissions. Range 256 to 2346 bytes.	`2346`
`vaps {vap1 ... vap`*n*`>`	Set the virtual access points carried on this physical access point.	No default.
`config deny-mac-list` **variables**		
`<mac_id>`	Enter a number to identify this entry.	No default.
`mac <mac>`	Enter the wireless MAC address to deny.	No default.

History

FortiOS v4.0 MR1 New.

Related commands

- wireless-controller vap

execute

The execute commands perform immediate operations on the FortiGate unit, including:

- Back up and restore the system configuration, or reset the unit to factory settings.
- Execute the run but not save feature
- Set the unit date and time.
- View and clear DHCP leases.
- Clear arp table entries.
- View and delete log messages. Delete old log files.
- Use ping or traceroute to diagnose network problems.
- Restart the router or the entire FortiGate unit.
- Update the antivirus and attack definitions on demand.
- Generate certificate requests and install certificates for VPN authentication.

This chapter contains the following sections:

backup

Back up the FortiGate configuration files, logs, or IPS user-defined signatures file to a TFTP or FTP server, USB disk, or a management station. Management stations can either be a FortiManager unit, or FortiGuard Analysis and Management Service. For more information, see "system fortiguard" on page 417 or "system central-management" on page 406.

When virtual domain configuration is enabled (in `system global`, `vdom-admin` is enabled), the content of the backup file depends on the administrator account that created it.

- A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin can restore the configuration from this file.
- When you back up the system configuration from a regular administrator account, the backup file contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

Syntax

```
execute backup config ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> [<password_str>]]
   [<backup_password_str>]
execute backup config management-station <comment_str>
execute backup config tftp <filename_str> <server_ipv4>
   [<backup_password_str>]
execute backup config usb <filename_str> [<backup_password_str>]
execute backup full-config ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> [<password_str>]]
   [<backup_password_str>]
execute backup full-config tftp <filename_str> <server_ipv4>
   [<backup_password_str>]
execute backup full-config usb <filename_str> [<backup_password_str>]
execute backup ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> [<password_str>]]
execute backup ipsuserdefsig tftp tftp <filename_str> <server_ipv4>
execute backup {disk | memory} alllogs ftp <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> <password_str>]
execute backup {disk | memory} alllogs tftp <server_ipv4>
execute backup {disk | memory} log ftp <server_ipv4[:port_int] |
   server_fqdn[:port_int]> <username_str> <password_str> {app-ctrl | event
   | ids | im | spam | virus | voip | webfilter}
execute backup {disk | memory} log tftp <server_ipv4> {app-ctrl | event |
   ids | im | spam | virus | voip | webfilter}
```

Variable	Description
`config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]`	Back up the system configuration to an FTP server. Optionally, you can specify a password to protect the saved data.
`config management-station <comment_str>`	Back up the system configuration to a configured management station. If you are adding a comment, do not add spaces, underscore characters (_), or quotation marks (“ “) or any other punctuation marks. For example, uploadedthetransparentmodeconfigfortheaccountingdepartmentwilluploadonadailybasis. The comment you enter displays in both the portal website and FortiGate web-based manager (**System** > **Maintenance** > **Revision**).
`config tftp <filename_str> <server_ipv4> [<backup_password_str>]`	Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data.
`config usb <filename_str> [<backup_password_str>]`	Back up the system configuration to a file on a USB disk. Optionally, you can specify a password to protect the saved data.
`full-config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>]`	Back up the full system configuration to a file on an FTP server. You can optionally specify a password to protect the saved data.
`full-config tftp <filename_str> <server_ipv4> [<backup_password_str>]`	Back up the full system configuration to a file on a TFTP server. You can optionally specify a password to protect the saved data.
`full-config usb <filename_str> [<backup_password_str>]`	Back up the full system configuration to a file on a USB disk. You can optionally specify a password to protect the saved data.
`ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> [<password_str>]]`	Backup IPS user-defined signatures to a file on an FTP server.
`ipsuserdefsig tftp tftp <filename_str> <server_ipv4>`	Back up IPS user-defined signatures to a file on a TFTP server.
`{disk | memory} alllogs ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]`	Back up either all memory or all hard disk log files for this VDOM to an FTP server. The disk option will only be available on FortiGate models that log to a hard disk. The file name has the form: <log_file_name>_<VDOM>_<date>_<time>
`{disk | memory} alllogs tftp <server_ipv4>`	Back up either all memory or all hard disk log files for this VDOM to a TFTP server. The disk option will only be available on FortiGate models that log to a hard disk. The file name has the form: <log_file_name>_<VDOM>_<date>_<time>
`{disk | memory} log ftp <server_ipv4[:port_int] | server_fqdn[:port_int]> <username_str> <password_str> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}`	Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option will only be available on FortiGate models that log to a hard disk.
`{disk | memory} log tftp <server_ipv4> {app-ctrl | event | ids | im | spam | virus | voip | webfilter}`	Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option will only be available on FortiGate models that log to a hard disk.

Example

This example shows how to backup the FortiGate unit system configuration to a file named `fgt.cfg` on a TFTP server at IP address 192.168.1.23.

```
execute backup config tftp fgt.cfg 192.168.1.23
```

History

FortiOS v2.80	Revised.
FortiOS v3.0	Added USB backup options.
FortiOS v3.0 MR1	Changed `backup log` from `<name> <tftp_ipv4>` to `<tftp_ipv4> <log_type>`.
FortiOS v3.0 MR3	`log` and `alllogs` now refer to either `disk` or `memory` as selected.
FortiOS v3.0 MR4	Added `full-config tftp` and `full-config usb`.
FortiOS v3.0 MR5	Added `config management-station`.
FortiOS v3.0 MR6	Added `ftp` to the commands.
FortiOS v3.0 MR7	Added ftp_username to `backup config ftp`. Fixed typo in `backup full-config tftp`.
FortiOS 4.0.0	Added the ability to back up all logs and individual log types to FTP servers as well as TFTP servers.

Related topics

- execute restore
- ips custom

batch

Execute a series of CLI commands.

Note: `execute batch` commands are controlled by the Maintenance (`mntgrp`) access control group.

Syntax

```
execute batch [<cmd_cue>]
```

where <cmd_cue> is one of:

- `end` - exit session and run the batch commands
- `lastlog` - read the result of the last batch commands
- `start` - start batch mode
- `status -` batch mode status reporting if batch mode is running or stopped

Example

To start batch mode:

```
execute batch start
Enter batch mode...
```

To enter commands to run in batch mode:

```
config system global
  set refresh 5
end
```

To execute the batch commands:

```
execute batch end
Exit and run batch commands...
```

History

FortiOS v3.0 MR1	New.
FortiOS v3.0 MR4	Control of `execute batch` commands in Maintenance (`mntgrp`) access control group.
FortiOS v3.0 MR5	Added `lastlog`.

central-mgmt

Update Central Management Service account information. Also used receive configuration file updates from an attached FortiManager unit.

Syntax

```
execute central-mgmt set-mgmt-id <management_id>
execute central-mgmt update
```

`set-mgmt-id` is used to change or initially set the management ID, or your account number for Central Management Services. This account ID must be set for the service to be enabled.

`update` is used to update your Central Management Service contract with your new management account ID. This command is to be used if there are any changes to your management service account.

`update` is also one of the steps in your FortiGate unit receiving a configuration file from an attached FortiManager unit. For more information, see “system central-management” on page 406.

Example

If you are registering with the Central Management Service for the first time, and your account number is 123456, you would enter the following:

```
execute central-mgmt set-mgmt-id 123456
execute central-mgmt update
```

History

FortiOS v3.0 MR5 New.

Related topics

- system central-management

cfg reload

Use this command to restore the saved configuration when the configuration change mode is `manual` or `revert`. This command has no effect if the mode is `automatic`, the default. The `set cfg-save` command in `system global` sets the configuration change mode.

When you reload the saved system configuration, the your session ends and the FortiGate unit restarts.

In the default configuration change mode, `automatic`, CLI commands become part of the saved unit configuration when you execute them by entering either next or end.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the FortiGate unit restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are saved automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. You set the timeout in `system global` using the `set cfg-revert-timeout` command.

Syntax

```
execute cfg reload
```

Example

This is sample output from the command when successful:

```
# exec cfg reload
configs reloaded. system will reboot.This is sample output from the command
   when not in runtime-only configuration mode:
# exec cfg reload
no config to be reloaded.
```

History

FortiOS v3.0 MR2 New.

Related topics

- execute cfg save
- system global

cfg save

Use this command to save configuration changes when the configuration change mode is `manual` or `revert`. If the mode is `automatic`, the default, all changes are added to the saved configuration as you make them and this command has no effect. The `set cfg-save` command in `system global` sets the configuration change mode.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the FortiGate unit restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are saved automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. To change the timeout from the default of 600 seconds, go to `system global` and use the `set cfg-revert-timeout` command.

Syntax

```
execute cfg save
```

Example

This is sample output from the command:

```
# exec cfg save
config saved.
```

This is sample output when not in runtime-only configuration mode. It also occurs when in runtime-only configuration mode and no changes have been made:

```
# exec cfg save
no config to be saved.
```

History

FortiOS v3.0 MR2 New.

Related topics

- execute cfg reload
- system global

clear system arp table

Clear all the entries in the arp table.

Syntax

```
exec clear system arp table
```

History

FortiOS v3.0 MR3 New.

Related topics

- execute router restart
- get router info routing-table
- get system arp

cli check-template-status

Reports the status of the secure copy protocol (SCP) script template.

Syntax

```
exec cli check-template-status
```

History

FortiOS v3.0 MR6 New.

cli status-msg-only

Enable standardized CLI error output messages. If executed, this command stops other debug messages from displaying in the current CLI session.

Syntax

```
exec cli status-msg-only <enable | disable>
```

The message format is:

```
[error code]: text message
```

There are two error categories: Keyword Error, and Data Error. The error code provides details about the type of error.

An ERROR message indicates that the command generated an error. A Keyword Error `[1000x]` indicates that the field or option is not supported, or the attempted command is not recognized. A Data Error `[2000x]` indicates that the data source is already in use.

Variable	Description
`status-msg-only <enable | disable>`	Enables standardized CLI error output messages.

History

FortiOS v3.0 MR5 New.

FortiOS v3.0 MR6 No longer sends OK message.

date

Get or set the system date.

Syntax

```
execute date [<date_str>]
```

`date_str` has the form `yyyy-mm-dd`, where

- `yyyy` is the year and can be `2001` to `2037`
- `mm` is the month and can be `01` to `12`
- `dd` is the day of the month and can be `01` to `31`

If you do not specify a date, the command returns the current system date. Shortened values, such as '06' instead of '2006' for the year or '1' instead of '01' for month or day, are not valid.

Example

This example sets the date to 17 September 2004:

```
execute date 2004-09-17
```

History

FortiOS v2.80 MR4 New.

FortiOS v3.0 MR1 `<date_str>` changed from mm/dd/yyyy format.

Related topics

- execute time

dhcp lease-clear

Clear all DHCP address leases.

Syntax

```
execute dhcp lease-clear
```

History

FortiOS v2.80 MR2	New.
FortiOS v3.0	Command name changed from `execute dhcpclear`.

Related topics

- execute dhcp lease-list
- system dhcp server
- system dhcp reserved-address

dhcp lease-list

Display DHCP leases on a given interface

Syntax

```
execute dhcp lease-list [interface_name]
```

If you specify an interface, the command lists only the leases issued on that interface. Otherwise, the list includes all leases issued by DHCP servers on the FortiGate unit.

If there are no DHCP leases in user on the FortiGate unit, an error will be returned.

History

FortiOS v2.90 New.

Related topics

- system dhcp server
- system dhcp reserved-address

disconnect-admin-session

Disconnect an administrator who is logged in.

Syntax

```
execute disconnect-admin-session <index_number>
```

To determine the index of the administrator that you want to disconnect, view the list of logged-in administrators by using the following command:

```
execute disconnect-admin-session ?
```

The list of logged-in administrators looks like this:

```
Connected:
INDEX   USERNAME     TYPE      FROM                TIME
0       admin        WEB       172.20.120.51       Mon Aug 14 12:57:23 2006
1       admin2       CLI       ssh(172.20.120.54)  Mon Aug 14 12:57:23 2006
```

Example

This example shows how to disconnect a logged in administrator.

```
execute disconnect-admin-session 1
```

History

FortiOS v2.90	New.
FortiOS v3.0 MR3	Changed `execute disconnect <index_number>` to `execute disconnect-admin-session <index_number>`. Deleted `get system logged-users` reference.

Related topics

- system mac-address-table
- get system info admin status

enter

Use this command to go from global commands to a specific virtual domain (VDOM).

Only available when virtual domains are enabled and you are in config global.

After you enter the VDOM, the prompt will not change from "`(global)`". However you will be in the VDOM with all the commands that are normally available in VDOMs.

Syntax

```
execute enter <vdom>
```

Use "?" to see a list of available VDOMs.

History

FortiOS v3.0 MR7 New.

factoryreset

Reset the FortiGate configuration to factory default settings.

Syntax

```
execute factoryreset
```

Caution: This procedure deletes all changes that you have made to the FortiGate configuration and reverts the system to its original configuration, including resetting interface addresses.

History

FortiOS v2.80 No changes.

Related topics

- execute backup
- execute reboot

firmware-list update

Use this command to update the list of firmware.

Syntax

```
execute firmware-list update
```

When the update is complete, the command reports:

```
Updating Image List. Done.
```

History

FortiOS v4.0 MR1 New.

formatlogdisk

Format the FortiGate hard disk to enhance performance for logging.

Syntax

```
execute formatlogdisk
```

Caution: This operation will erase all quarantine files and logging data on the hard disk.

History

FortiOS v2.80 No change.

fortiguard-log update

Update the FortiGuard Analysis and Management Service contract.

Syntax

```
execute fortiguard-log update
```

History

FortiOS v3.0 MR4 New.

Related topics

- system fortiguard
- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter

fsae refresh

Use this command to manually refresh user group information from Directory Service servers connected to the FortiGate unit using the Fortinet Server Authentication Extensions (FSAE).

Syntax

```
execute fsae refresh
```

History

FortiOS v3.0	New.
FortiOS v3.0 MR7	Changed Active Directory to Directory Service.

Related topics

- user fsae

ha disconnect

Use this command to disconnect a FortiGate unit from a functioning cluster. You must specify the serial number of the unit to be disconnected. You must also specify an interface name and assign an IP address and netmask to this interface of the disconnected unit. You can disconnect any unit from the cluster even the primary unit. After the unit is disconnected the cluster responds as if the disconnected unit has failed. The cluster may renegotiate and may select a new primary unit.

To disconnect the unit from the cluster, the `execute ha disconnect` command sets the HA `mode` of the disconnected unit to standalone. In addition, all interface IP addresses of the disconnected unit are set to 0.0.0.0. The interface specified in the command is set to the IP address and netmask that you specify in the command. In addition all management access to this interface is enabled. Once the FortiGate unit is disconnected you can use SSH, telnet, HTTPS, or HTTP to connect to and manage the FortiGate unit.

Syntax

```
execute ha disconnect <cluster-member-serial_str> <interface_str>
   <address_ipv4> <address_ipv4mask>
```

Variable	Description
`cluster-member-serial_str`	The serial number of the cluster unit to be disconnected.
`interface_str`	The name of the interface to configure. The command configures the IP address and netmask for this interface and also enables all management access for this interface.

Example

This example shows how to disconnect a cluster unit with serial number FGT5002803033050. The internal interface of the disconnected unit is set to IP address 1.1.1.1 and netmask 255.255.255.0.

```
execute ha disconnect FGT5002803033050 internal 1.1.1.1 255.255.255.0
```

History

FortiOS v3.0 New

Related topics

- execute ha manage
- execute ha synchronize
- system ha

ha manage

Use this command from the CLI of a FortiGate unit in an HA cluster to log into the CLI of another unit in the cluster. Usually you would use this command from the CLI of the primary unit to log into the CLI of a subordinate unit. However, if you have logged into a subordinate unit CLI, you can use this command to log into the primary unit CLI, or the CLI of another subordinate unit.

You can use CLI commands to manage the cluster unit that you have logged into. If you make changes to the configuration of any cluster unit (primary or subordinate unit) these changes are synchronized to all cluster units.

Syntax

```
execute ha manage <cluster-index>
```

Variable	Description
cluster-index	The cluster index is assigned by the FortiGate Clustering Protocol according to cluster unit serial number. The cluster unit with the highest serial number has a cluster index of 0. The cluster unit with the second highest serial number has a cluster index of 1 and so on. Enter ? to list the cluster indexes of the cluster units that you can log into. The list does not show the unit that you are already logged into.

Example

This example shows how to log into a subordinate unit in a cluster of three FortiGate units. In this example you have already logged into the primary unit. The primary unit has serial number FGT3082103000056. The subordinate units have serial numbers FGT3012803021709 and FGT3082103021989.

```
execute ha manage ?
   <id>    please input slave cluster index.
   <0>     Subsidary unit FGT3012803021709
   <1>     Subsidary unit FGT3082103021989
```

Type 0 and press enter to connect to the subordinate unit with serial number FGT3012803021709. The CLI prompt changes to the host name of this unit. To return to the primary unit, type `exit`.

From the subordinate unit you can also use the `execute ha manage` command to log into the primary unit or into another subordinate unit. Enter the following command:

```
execute ha manage ?
   <id>    please input slave cluster index.
   <1>     Subsidary unit FGT3082103021989
   <2>     Subsidary unit FGT3082103000056
```

Type 2 and press enter to log into the primary unit or type 1 and press enter to log into the other subordinate unit. The CLI prompt changes to the host name of this unit.

History

FortiOS v2.80 Unchanged.

FortiOS v3.0 Unchanged.

Related topics

- execute ha disconnect, execute ha synchronize
- system ha

ha synchronize

Use this command from a subordinate unit in an HA cluster to manually synchronize its configuration with the primary unit. Using this command you can synchronize the following:

- Configuration changes made to the primary unit (normal system configuration, firewall configuration, VPN configuration and so on stored in the FortiGate configuration file),
- Antivirus engine and antivirus definition updates received by the primary unit from the FortiGuard Distribution Network (FDN),
- IPS attack definition updates received by the primary unit from the FDN,
- Web filter lists added to or changed on the primary unit,
- Email filter lists added to or changed on the primary unit,
- Certification Authority (CA) certificates added to the primary unit,
- Local certificates added to the primary unit.

You can also use the `start` and `stop` fields to force the cluster to synchronize its configuration or to stop a synchronization process that is in progress.

Syntax

```
execute ha synchronize {config| avupd| attackdef| weblists| emaillists|
   ca| localcert| ase | all | start | stop}
```

Variable	Description
`config`	Synchronize the FortiGate configuration.
`avupd`	Synchronize the antivirus engine and antivirus definitions.
`attackdef`	Synchronize attack definitions.
`weblists`	Synchronize web filter lists.
`emaillists`	Synchronize email filter lists.
`ca`	Synchronize CA certificates.
`localcert`	Synchronize local certificates.
`ase`	Synchronize the antispam engine and antispam rule sets.
`all`	Synchronize all of the above.
`start`	Start synchronizing the cluster configuration.
`stop`	Stop the cluster from completing synchronizing its configuration.

Example

From the CLI of a subordinate unit, use the following commands to synchronize the antivirus and attack definitions on the subordinate FortiGate unit with the primary unit after the FDN has pushed new definitions to the primary unit.

```
execute ha synchronize avupd
execute ha synchronize attackdef
```

History

FortiOS v2.80 MR6 Added `start` and `stop` fields.

FortiOS v3.0 Unchanged.

FortiOS v4.0 Added `ase` field.

Related topics

- execute ha disconnect
- execute ha manage
- system ha

interface dhcpclient-renew

Renew the DHCP client for the specified DHCP interface and close the CLI session. If there is no DHCP connection on the specified port, there is no output.

Syntax

```
execute interface dhcpclient-renew <port>
```

Example

This is the output for renewing the DHCP client on port1 before the session closes:

```
# exec interface dhcpclient-renew port1
renewing dhcp lease on port1
```

History

FortiOS v3.0 MR2 New. Replaces the old `connect-enable` command

Related topics

- execute dhcp lease-list

interface pppoe-reconnect

Reconnect to the PPPoE service on the specified PPPoE interface and close the CLI session. If there is no PPPoE connection on the specified port, there is no output.

Syntax

```
execute interface pppoe-reconnect <port>
```

History

FortiOS v3.0 MR2 New. Replaces the old `connect-enable` command

Related topics

- execute modem dial
- execute modem hangup

log delete-all

Use this command to clear all log entries in memory and current log files on hard disk. If your FortiGate unit has no hard disk, only log entries in system memory will be cleared. You will be prompted to confirm the command.

Syntax

```
execute log delete-all
```

History

FortiOS v3.0 MR2 No change.

Related topics

- execute log delete-rolled
- execute log display
- execute log filter
- execute log list

log delete-rolled

Use this command to delete rolled log files.

Syntax

```
execute log delete-rolled <category> <start> <end>
```

Variable	Description
<category>	Enter the category of rolled log files that you want to delete: • traffic • event • virus • webfilter • attack • spam • content • im • voip • dlp • app-crtl The <category> must be one of the above categories. The FortiGate unit can only delete one category at a time.
<start>	Enter the number of the first log to delete. If you are deleting multiple rolled log files, you must also enter a number for end. The <start> and <end> values represent the range of rolled log files to delete. If <end> is not specified, only the <start> log number is deleted.
<end>	Enter the number of the last log to delete, if you are deleting multiple rolled log files. The <start> and <end> values represent the range of rolled log files to delete. If <end> is not specified, only the <start> log number is deleted.

Example

The following deletes all event rolled logs from 1 to 50.

```
execute log delete-rolled event 1 50
```

History

FortiOS v3.0 MR2 No change.

FortiOS v4.0 Added dlp and app-crtl fields.

Related topics

- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
- execute log filter
- execute log delete-all

log display

Use this command to display log messages that you have selected with the `execute log filter` command.

Syntax

```
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the commands

```
execute log filter start-line 1
execute log display
```

You can restore the log filters to their default values using the command

```
execute log filter reset
```

History

FortiOS v2.90 New.

Related topics

- execute log filter

log filter

Use this command to select log messages for viewing or deletion. You can view one log category on one device at a time. Optionally, you can filter the messages to select only specified date ranges or severities of log messages. For traffic logs, you can filter log messages by source or destination IP address.

Commands are cumulative. If you omit a required variable, the command displays the current setting.

Use as many `execute log filter` commands as you need to define the log messages that you want to view.

```
execute log filter category <category_name>
execute log filter device {disk | memory}
execute log filter dump
execute log filter field <name>
execute log filter ha-member <unitsn_str>
execute log filter reset
execute log filter rolled_number <number>
execute log filter start-line <line_number>
execute log filter view-lines <count>
```

Variable	Description	Default
`category <category_name>`	Enter the type of log you want to select, one of: • traffic • event • virus • webfilter • spam • attack • content • im • voip • dlp • app-crtl	`event`
`device {disk | memory}`	Device where the logs are stored.	`disk`
`dump`	Display current filter settings.	No default.
`field <name>`	Press Enter to view the fields that are available for the associated category. Enter the fields you want, using commas to separate multiple fields.	No default.
`ha-member <unitsn_str>`	Select logs from the specified HA cluster member. Enter the serial number of the unit.	
`reset`	Execute this command to reset all filter settings.	No default.
`rolled_number <number>`	Select logs from rolled log file. 0 selects current log file.	`0`
`start-line <line_number>`	Select logs starting at specified line number.	`1`
`view-lines <count>`	Set lines per view. Range: 5 to 1000	`10`

History

FortiOS v4.0 Added `dlp` and `app-crtl` fields in `category`.

FortiOS v4.0 MR1 Added `ha-member`. Changed `lines-per-view` to `view-lines` and `list` to `dump`.

Related topics

- execute log display

log fortianalyzer test-connectivity

Use this command to test the connection to the FortiAnalyzer unit. This command is available only when FortiAnalyzer is configured.

Syntax

```
execute log fortianalyzer test-connectivity
```

Example

When FortiAnalyzer is connected, the output looks like this:

```
FortiAnalyzer Host Name: FortiAnalyzer-800B
FortiGate Device ID: FG50B3G06500085
Registration: registered
Connection: allow
Disk Space (Used/Allocated): 468/1003 MB
Total Free Space: 467088 MB
Log: Tx & Rx
Report: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
```

When FortiAnalyzer is not connected, the output is: `Connect Error`

History

FortiOS v3.0 New.

Related topics

- log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting

log list

You can view the list of current and rolled log files on the console. The list shows the file name, size and timestamp.

Syntax

```
execute log list <category>
```

<category> must be one of: `traffic`, `event`, `virus`, `webfilter`, `attack`, `spam`, `content`, `im`, `voip`, `dlp` and `app-ctrl`.

Example

The output looks like this:

```
elog                  8704    Fri March 6 14:24:35 2009
elog.1                1536    Thu March 5 18:02:51 2009
elog.2               35840    Wed March 4 22:22:47 2009
```

At the end of the list, the total number of files in the category is displayed. For example:

```
501 event log file(s) found.
```

History

FortiOS 4.0 Added the `category` options, `dlp` and `app-ctrl`.

Related topics

- execute log delete-rolled

log roll

Use this command to roll all log files.

Syntax

```
execute log roll
```

History

FortiOS v3.0 New.

Related topics

- execute log delete-rolled

modem dial

Dial the modem.

The dial command dials the accounts configured in `config system modem` until it makes a connection or it has made the maximum configured number of redial attempts.

This command applies only to models 50A, 60, 60M and 60-WiFi and is effective only if the modem is in Standalone mode.

Syntax

```
execute modem dial
```

History

FortiOS v2.80 New

Related topics

- system modem
- execute modem hangup

modem hangup

Hang up the modem.

This command applies only to models 50A, 60, 60M and 60-WiFi and is effective only if the modem is in Standalone mode.

Syntax

```
execute modem hangup
```

History

FortiOS v2.80 New

Related topics

- system modem
- execute modem dial

modem trigger

This command sends a signal to the modem daemon, which causes the state machine to re-evaluate its current state. If for some reason the modem should be connected but isn't, then it will trigger a redial. If the modem should not be connected but is, this command will cause the modem to disconnect.

Syntax

```
execute modem trigger
```

History

FortiOS v4.0 New

Related topics

- execute modem dial
- execute modem hangup

mrouter clear

Clear multicast routes, RP-sets, IGMP membership records or routing statistics.

Syntax

Clear IGMP memberships:

```
execute mrouter clear igmp-group {{<group-address>} <interface-name>}
execute mrouter clear igmp-interface <interface-name>
```

Clear multicast routes:

```
execute mrouter clear <route-type> {<group-address> {<source-address>}}
```

Clear PIM-SM RP-sets learned from the bootstrap router (BSR):

```
execute mrouter clear sparse-mode-bsr
```

Clear statistics:

```
execute mrouter clear statistics {<group-address> {<source-address>}}
```

Variable	Description
<interface-name>	Enter the name of the interface on which you want to clear IGMP memberships.
<group-address>	Optionally enter a group address to limit the command to a particular group.
<route-type>	Enter one of: • dense-routes - clear only PIM dense routes • multicast-routes - clear all types of multicast routes • sparse-routes - clear only sparse routes
<source-address>	Optionally, enter a source address to limit the command to a particular source address. You must also specify group-address.

History

FortiOS v3.0	New
FortiOS v4.0 MR1	routes changed to multicast-routes.

i

Related topics

- router multicast
- get router info bgp

ping

Send an ICMP echo request (ping) to test the network connection between the FortiGate unit and another network device.

Syntax

```
execute ping {<address_ipv4> | <host-name_str>}
```

<host-name_str> should be an IP address, or a fully qualified domain name.

Example

This example shows how to ping a host with the IP address 172.20.120.16.

```
#execute ping 172.20.120.16

PING 172.20.120.16 (172.20.120.16): 56 data bytes
64 bytes from 172.20.120.16: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.20.120.16: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=4 ttl=128 time=0.2 ms

--- 172.20.120.16 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

History

FortiOS v2.80 No change.

FortiOS v3.0 No change.

Related topics

- execute ping-options, ping6-options
- execute ping6
- execute traceroute

ping-options, ping6-options

Set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiGate unit and another network device.

Syntax

```
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats>
execute ping-options source {auto | <source-intf_ip>}
execute ping-options timeout <seconds>
execute ping-options tos <service_type>
execute ping-options ttl <hops>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Variable	Description	Default
`data-size <bytes>`	Specify the datagram size in bytes.	56
`df-bit {yes | no}`	Set `df-bit` to `yes` to prevent the ICMP packet from being fragmented. Set `df-bit` to `no` to allow the ICMP packet to be fragmented.	no
`pattern <2-byte_hex>`	Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the `data_size` parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	No default.
`repeat-count <repeats>`	Specify how many times to repeat ping.	5
`source {auto | <source-intf_ip>}`	Specify the FortiGate interface from which to send the ping. If you specify `auto`, the FortiGate unit selects the source address and interface based on the route to the `<host-name_str>` or `<host_ip>`. Specifying the IP address of a FortiGate interface tests connections to different network segments from the specified interface.	auto
`timeout <seconds>`	Specify, in seconds, how long to wait until ping times out.	2
`tos <service_type>`	Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted. • lowdelay = minimize delay • throughput = maximize throughput • reliability = maximize reliability • lowcost = minimize cost	0
`ttl <hops>`	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	64
`validate-reply {yes | no}`	Select `yes` to validate reply data.	no
`view-settings`	Display the current ping-option settings.	No default

Example

Use the following command to increase the number of pings sent.

```
execute ping-options repeat-count 10
```

Use the following command to send all pings from the FortiGate interface with IP address 192.168.10.23.

```
execute ping-options source 192.168.10.23
```

History

FortiOS v2.80 No change.

Related topics

- execute ping
- execute ping6
- execute traceroute
- system tos-based-priority

ping6

Send an ICMP echo request (ping) to test the network connection between the FortiGate unit and an IPv6 capable network device.

Syntax

```
execute ping6 {<address_ipv6> | <host-name_str>}
```

Example

This example shows how to ping a host with the IPv6 address `12AB:0:0:CD30:123:4567:89AB:CDEF`.

```
execute ping6 12AB:0:0:CD30:123:4567:89AB:CDEF
```

History

FortiOS v2.80 New.

Related topics

- execute ping
- execute ping-options, ping6-options
- router static6

reboot

Restart the FortiGate unit.

Caution: Abruptly powering off your FortiGate unit may corrupt its configuration. Using the reboot and shutdown options here or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute reboot <comment “comment_string”>
```

<comment “comment_string”> allows you to optionally add a message that will appear in the hard disk log indicating the reason for the reboot. If the message is more than one word it must be enclosed in quotes.

Example

This example shows the reboot command with a message included.

```
execute reboot comment “December monthly maintenance”
```

History

FortiOS v2.80	Unchanged.
FortiOS v3.0 MR4	Added `comment` field.

Related topics

- execute backup
- execute factoryreset
- execute shutdown

restore

Use this command to

- restore the configuration from a file
- change the FortiGate firmware
- change the FortiGate backup firmware
- restore an IPS custom signature file

When virtual domain configuration is enabled (in `system global`, `vdom-admin` is enabled), the content of the backup file depends on the administrator account that created it.

- A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin account can restore the configuration from this file.
- A backup file from a regular administrator account contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

Syntax

```
execute restore ase ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore ase tftp <filename_str> <server_ipv4[:port_int]>
execute restore av ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore av tftp <filename_str> <server_ipv4[:port_int]>
execute restore config ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> <password_str>]
   [<backup_password_str>]
execute restore config management-station {normal | template | script}
   <rev_int>
execute restore config tftp <filename_str> <server_ipv4>
   [<backup_password_str>]
execute restore config usb <filename_str> [<backup_password_str>]
execute restore image ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore image management-station <version_int>
execute restore image tftp <filename_str> <server_ipv4>
execute restore image usb <filename_str>
execute restore ips ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore ips tftp <filename_str> <server_ipv4>
execute restore ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore ipsuserdefsig tftp <filename_str> <server_ipv4>
execute restore secondary-image ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore secondary-image tftp <filename_str> <server_ipv4>
execute restore secondary-image usb <filename_str>
execute restore forticlient tftp <filename_str> <server_ipv4>
```

Variable	Description
`ase ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]`	Restore the antispam engine. Download the restore file from an FTP server. The user and password to access the FTP server are only necessary if the server requires them
`ase tftp <filename_str> <server_ipv4[:port_int]>`	Restore the antispam engine. Download the restore file from a TFTP server.
`av ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]`	Download the antivirus database file from an FTP server to the FortiGate unit.
`av tftp <filename_str> <server_ipv4[:port_int]>`	Download the antivirus database file from a TFTP server to the FortiGate unit.
`config ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>] [<backup_password_str>]`	Restore the system configuration from an FTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password.
`config management-station {normal | template | script} <rev_int>`	Restore the system configuration from the central management server. The new configuration replaces the existing configuration, including administrator accounts and passwords. `rev_int` is the revision number of the saved configuration to restore. Enter `0` for the most recent revision.
`config tftp <filename_str> <server_ipv4> [<backup_password_str>]`	Restore the system configuration from a file on a TFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password.
`config usb <filename_str> [<backup_password_str>]`	Restore the system configuration from a file on a USB disk. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password.
`image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]`	Download a firmware image from an FTP server to the FortiGate unit. The FortiGate unit reboots, loading the new firmware. This command is not available in multiple VDOM mode.
`image management-station <version_int>`	Download a firmware image from the central management station. This is available if you have configured a FortiManager unit as a central management server. This is also available if your account with FortiGuard Analysis and Management Service allows you to upload firmware images.
`image tftp <filename_str> <server_ipv4>`	Download a firmware image from a TFTP server to the FortiGate unit. The FortiGate unit reboots, loading the new firmware. This command is not available in multiple VDOM mode.
`image usb <filename_str>`	Download a firmware image from a USB disk to the FortiGate unit. The FortiGate unit reboots, loading the new firmware.
`ips ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]`	Download the IPS database file from an FTP server to the FortiGate unit.
`ips tftp <filename_str> <server_ipv4>`	Download the IPS database file from a TFTP server to the FortiGate unit.

Variable	Description
`ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]`	Restore IPS custom signature file from an FTP server. The file will overwrite the existing IPS custom signature file.
`ipsuserdefsig tftp <filename_str> <server_ipv4>`	Restore an IPS custom signature file from a TFTP server. The file will overwrite the existing IPS custom signature file.
`secondary-image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]`	Download a firmware image from an FTP server as the backup firmware of the FortiGate unit. This is available only on models that support backup firmware images.
`secondary-image tftp <filename_str> <server_ipv4>`	Download a firmware image from a TFTP server as the backup firmware of the FortiGate unit. This is available only on models that support backup firmware images.
`secondary-image usb <filename_str>`	Download a firmware image from a USB disk as the backup firmware of the FortiGate unit. The unit restarts when the upload is complete. This is available only on models that support backup firmware images.
`forticlient tftp <filename_str> <server_ipv4>`	Download the FortiClient image from a TFTP server to the FortiGate unit. The filename must have the format: FortiClientSetup_*versionmajor.versionminor.build*.exe. For example, FortiClientSetup.4.0.377.exe.

Example

This example shows how to upload a configuration file from a TFTP server to the FortiGate unit and restart the FortiGate unit with this configuration. The name of the configuration file on the TFTP server is `backupconfig`. The IP address of the TFTP server is 192.168.1.23.

```
execute restore config tftp backupconfig 192.168.1.23
```

History

FortiOS v2.80	Revised.
FortiOS v3.0	Added USB restore options and secondary-image restoration. Removed allconfig option.
FortiOS v3.0 MR2	Added FTP restore option.
FortiOS v3.0 MR4	Added `av`, `forticlient`, `ips` fields.
FortiOS v3.0 MR5	Added config management-station
FortiOS v3.0 MR6	Added `ftp` to all fields except `forticlient`.
FortiOS v4.0.0	Added `ase ftp` and `ase tftp`.

Related topics

- execute backup
- ips custom

router clear bfd session

Use this command to clear bi-directional forwarding session.

Syntax

```
execute router clear bfd session <src_ip> <dst_ip> <interface>
```

Variable	Description
<src_ip>	Select the source IP address of the session.
<dst_ip>	Select the destination IP address of the session.
<interface>	Select the interface for the session.

History

FortiOS v3.0 MR4 New.

Related topics

- router bgp

router clear bgp

Use this command to clear BGP peer connections.

Syntax

```
execute router clear bgp all [soft] [in | out]
execute router clear bgp as <as_number> [soft] [in | out]
execute router clear bgp dampening {ip_address | ip/netmask}
execute router clear bgp external {in prefix-filter} [soft] [in | out]
execute router clear bgp flap-statistics {ip_address | ip/netmask}
execute router clear bgp ip <ip_address> [soft] [in | out]
```

Variable	Description
`all`	Clear all BGP peer connections.
`as <as_number>`	Clear BGP peer connections by AS number.
`dampening {ip_address | ip/netmask}`	Clear route flap dampening information for peer or network.
`external {in prefix-filter}`	Clear all external peers.
`ip <ip_address>`	Clear BGP peer connections by IP address.
`peer-group`	Clear all members of a BGP peer-group.
`[in | out]`	Optionally limit clear operation to inbound only or outbound only.
`flap-statistics {ip_address | ip/netmask}`	Clear flap statistics for peer or network.
`soft`	Do a soft reset that changes the configuration but does not disturb existing sessions.

History

FortiOS v2.80 MR2 New.

FortiOS v3.0 MR1 Added flap-statistics field.

Related topics

- router bgp

router clear ospf process

Use this command to clear and restart the OSPF router.

Syntax

IPv4:

```
execute router clear ospf process
```

IPv6:

```
execute router clear ospf6 process
```

History

FortiOS v3.0 MR1 New.

Related topics

- router ospf

router restart

Use this command to restart the routing software.

Syntax

```
execute router restart
```

History

FortiOS v2.80 MR2 New.

Related topics

- router

scsi-dev

Use this command as part of a WAN optimization configuration to edit FortiGate SCSI devices that can include internal high-capacity hard drives, AMC module hard drives, and SAS devices. Unless you have special requirements, you do not need to change the SCSI device configuration unless you want to use more than one SCSI device for WAN optimization.

To configure SCSI devices for WAN optimization you:

1. Use the `execute scsi-dev partition` command to create and edit partitions.
2. Use the `execute scsi-dev storage` command to create WAN optimization storages. WAN optimization storages are logical parts of a partition used by WAN optimization to store the byte cache and web cache databases. You can create multiple storages but only two of then are used at a time; one for byte caching and one for web caching. You cannot use the same storage for both byte caching and web caching. You can add more than one storage to a partition.
3. Use the `config wanopt cache-storage` command to configure the storages to use for byte caching and web caching.

You can use the `show wanopt storage` command to view the storages that you have added. You can also use the `config wanopt storage` command to change the storage sizes. See "wanopt storage" on page 651.

See *WAN Optimization, Web Cache, and Web Proxy User Guide* for example of using the `execute scsi-dev` command.

Syntax

```
execute scsi-dev list
execute scsi-dev partition create <device_ref_int> <partition_size_int>
execute scsi-dev partition delete <partition_ref_int>
execute scsi-dev partition resize <partition_ref_int> <partition_size_int>
execute scsi-dev storage <partition_ref_int> <storage_size_int>
   <storage_name_str>
```

Variable	Description
`list`	List the SCSI devices and partitions. The list displays device reference numbers `<device_ref_int>`, partition reference numbers `<partition_ref_int>`, and partition sizes `<partition_size_int>`.
`partition create`	Create new SCSI device partitions.
`partition delete`	Delete SCSI device partitions.
`partition resize`	Expand or shrink a SCSI device partition. Only the last partition on a device can be resized.
`<device_ref_int>`	SCSI device reference number displayed by the `execute scsi-dev` list command. These numbers uniquely identify each SCSI device.
`<partition_size_int>`	The size of a partition in Mbytes.
`<partition_ref_int>`	Partition reference number displayed by the `execute scsi-dev` list command. These numbers uniquely identify each SCSI device partition.
`storage`	Add WAN optimization storages. The first time you add a storage to a partition using the `execute scsi-dev storage` command the partition is labelled with a random string (for example, `77A2A1AB1D0EF8B7`). This label is used for all storages added to a given partition. A different label is created for each partition. The labels appear when you use the `execute scsi-dev list` command to list the partitions.
`<storage_size_int>`	The size of a WAN optimization storage in Mbytes. The storage can be from 16 Mbytes up to the size of the partition.
`<storage_name_str>`	The name of the WAN optimization storage.

Examples

Use the following command to list the SCSI devices for a FortiGate unit that includes a FortiGate-ASM-S08 module.

```
#execute scsi-dev list

Device 1          492.0 MB      ref: 0         (Vendor:    Model: USB DISK 2.0
   Rev: PMAP)
  partition 1      39.1 MB       ref: 1          label: <none>
  partition 2      39.1 MB       ref: 2          label: <none>
  partition 3      39.1 MB       ref: 3          label: <none>

Device 2           74.5 GB       ref: 16       (Vendor: ATA Model: FUJITSU MH
W2080B Rev: 0)
  partition 1      74.5 GB       ref: 17         label: 404913186405899C
```

In this example, the device reference number for the hard disk on the FortiGate-ASM-S08 module is 16 and the partition reference number for the partition on this hard disk is 17. The label `404913186405899C` for partition ref 17 indicates that WAN optimization storages have been added to this partition.

Use the following command to add a WAN optimization storage named is `WAN_sto_1` to partition reference number 17. The storage size is 20 Mbytes.

```
execute scsi-dev storage 17 20 WAN_sto_1
Storage created;  size: 20MB  signature: WAN-sto_1-404913186405899C
```

History

FortiOS v4.0 New.

send-fds-statistics

Use this command to send an FDS statistics report now, without waiting for the FDS statistics report interval to expire.

Syntax

```
execute send-fds-statistics
```

History

FortiOS v3.0 MR6 New.

set-next-reboot

Use this command to start the FortiGate unit with primary or secondary firmware after the next reboot. This command is useful only on models numbered 100 and higher which are able to store two firmware images. By default, the FortiGate unit loads the firmware from the primary partition.

VDOM administrators do not have permission to run this command. It must be executed by a super administrator.

Syntax

```
execute set-next-reboot {primary | secondary}
```

History

FortiOS v3.0	New.
FortiOS v3.0 MR3	VDOM administrators can't run this command.

Related topics

- execute reboot
- execute shutdown

sfp-mode-sgmii

Change the SFP mode for an NP2 card to SGMII. By default when an AMC card is inserted the SFP mode is set to SERDES mode by default.

If a configured NP2 card is removed and re-inserted, the SFP mode goes back to the default.

In these situations, the `sfpmode-sgmii` command will change the SFP mode from SERDES to SGMII for the interface specified.

Syntax

```
execute sfpmode-sgmii <interface>
```

<interface> is the NP2 interface where you are changing the SFP mode.

History

FortiOS v3.0 MR7 New.

shutdown

Shut down the FortiGate unit now. You will be prompted to confirm this command.

Caution: Abruptly powering off your FortiGate unit may corrupt its configuration. Using the reboot and shutdown options here or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute shutdown [comment <comment_string>]
```

`comment` is optional but you can use it to add a message that will appear in the event log message that records the shutdown. The `comment` message of the does not appear on the Alert Message console. If the message is more than one word it must be enclosed in quotes.

Example

This example shows the reboot command with a message included.

```
execute shutdown comment “emergency facility shutdown”
```

An event log message similar to the following is recorded:

```
2009-09-08 11:12:31 critical admin 41986 ssh(172.20.120.11) shutdown User
admin shutdown the device from ssh(172.20.120.11). The reason is 'emergency
facility shutdown'
```

History

FortiOS v2.80 MR8 New.

FortiOS v3.0 MR4 Added `comment`.

Related topics

- execute factoryreset
- execute reboot

ssh

Use this command to establish an ssh session with another system.

Syntax

```
execute ssh <destination>
```

`<destination>` - the destination in the form user@ip or user@host.

Example

```
execute ssh admin@172.20.120.122
```

To end an ssh session, type `exit`:

```
FGT-6028030112 # exit
Connection to 172.20.120.122 closed.
FGT-8002805000 #
```

History

FortiOS v3.0 MR3 New.

Related topics

- execute ping
- execute traceroute
- system interface

telnet

Use telnet client. You can use this tool to test network connectivity.

Syntax

```
execute telnet <telnet_ipv4>
```

`<telnet_ipv4>` is the address to connect with.

Type `exit` to close the telnet session.

History

FortiOS v3.0 New.

Related topics

- execute ping
- execute traceroute
- system interface

time

Get or set the system time.

Syntax

```
execute time [<time_str>]
```

`time_str` has the form `hh:mm:ss`, where

- `hh` is the hour and can be `00` to `23`
- `mm` is the minutes and can be `00` to `59`
- `ss` is the seconds and can be `00` to `59`

If you do not specify a time, the command returns the current system time.

You are allowed to shorten numbers to only one digit when setting the time. For example both 01:01:01 and 1:1:1 are allowed.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

History

FortiOS v2.80 MR4 New.

Related topics

- execute date

traceroute

Test the connection between the FortiGate unit and another network device, and display information about the network hops between the device and the FortiGate unit.

Syntax

```
execute traceroute {<ip_address> | <host-name>}
```

Example

This example shows how to test the connection with http://docs.forticare.com. In this example the traceroute command times out after the first hop indicating a possible problem.

```
#execute traceoute docs.forticare.com
traceroute to docs.forticare.com (65.39.139.196), 30 hops max, 38 byte packets
 1  172.20.120.2 (172.20.120.2)  0.324 ms  0.427 ms  0.360 ms
 2  * * *
```

If your FortiGate unit is not connected to a working DNS server, you will not be able to connect to remote host-named locations with traceroute.

History

FortiOS v2.80 No change.

Related topics

- execute ping
- execute ping-options, ping6-options

update-ase

Use this command to manually initiate the antispam engine and rules update..

Syntax

```
execute update-ase
```

History

FortiOS 4.0 New

Related topics

- execute update-now

update-av

Use this command to manually initiate the virus definitions and engines update. To update both virus and attack definitions, use the `execute update-now` command.

Syntax

```
execute update-av
```

History

FortiOS v3.0 MR2 New

Related topics

- execute update-now
- system autoupdate override
- system autoupdate push-update
- system autoupdate schedule

update-ips

Use this command to manually initiate the Intrusion Prevention System (IPS) attack definitions and engine update. To update both virus and attack definitions, use the `execute update-now` command.

Syntax

```
execute update-ips
```

History

FortiOS v3.0 MR2 New.

FortiOS v3.0 MR4 Command name changed execute update-ids to execute update-ips.

Related topics

- execute update-now
- system autoupdate override
- system autoupdate override
- system autoupdate push-update
- system autoupdate schedule

update-now

Use this command to manually initiate both virus and attack definitions and engine updates. To initiate only virus or attack definitions, use the `execute update-av` or `execute update-ids` command respectively.

Syntax

```
execute update-now
```

History

FortiOS v2.80 Revised.

Related topics

- execute update-ase
- execute update-ips
- system autoupdate override
- system autoupdate push-update
- system autoupdate schedule

upd-vd-license

Use this command to enter a Virtual Domain (VDOM) license key.

If you have a FortiGate-3016A/B unit or higher, you can purchase a license key from Fortinet to increase the maximum number of VDOMs to 25, 50, 100 or 500. By default, FortiGate units support a maximum of 10 VDOMs.

This command is available only on FortiGate-3016A/B units and higher.

Note: . FortiGate-620B units do not support VDOMs.

Syntax

```
execute upd-vd-license <license_key>
```

Variable	Description
<license_key>	The license key is a 32-character string supplied by Fortinet. Fortinet requires your unit serial number to generate the license key.

History

FortiOS v3.0 New.

usb-disk

Use these commands to manage your USB disks.

Syntax

```
execute usb-disk delete <filename>
execute usb-disk format
execute usb-disk list
execute usb-disk rename <old_name> <new_name>
```

Variable	Description
`delete <filename>`	Delete the named file from the USB disk.
`format`	Format the USB disk.
`list`	List the files on the USB disk.
`rename <old_name> <new_name>`	Rename a file on the USB disk.

History

FortiOS v3.0 New.

Related topics

- execute backup
- execute restore

vpn certificate ca

Use this command to import a CA certificate from a TFTP or SCEP server to the FortiGate unit, or to export a CA certificate from the FortiGate unit to a TFTP server.

Before using this command you must obtain a CA certificate issued by a CA.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The CA certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

Note: VPN peers must use digital certificates that adhere to the X.509 standard.

Note: Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

```
execute vpn certificate ca export tftp <certificate-name_str>
   <file-name_str> <tftp_ip>
execute vpn certificate ca import auto <ca_server_url> <ca_identifier_str>
execute vpn certificate ca import tftp <file-name_str> <tftp_ip>
```

Variable	Description
`import`	Import the CA certificate from a TFTP server to the FortiGate unit.
`export`	Export or copy the CA certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
`<certificate-name_str>`	Enter the name of the CA certificate.
`<file-name_str>`	Enter the file name on the TFTP server.
`<tftp_ip>`	Enter the TFTP server address.
`auto`	Retrieve a CA certificate from a SCEP server.
`tftp`	Import the CA certificate to the FortiGate unit from a file on a TFTP server (local administrator PC).
`<ca_server_url>`	Enter the URL of the CA certificate server.
`<ca_identifier_str>`	CA identifier on CA certificate server (optional).

Examples

Use the following command to import the CA certificate named `trust_ca` to the FortiGate unit from a TFTP server with the address `192.168.21.54`.

```
execute vpn certificate ca import trust_ca 192.168.21.54
```

History

FortiOS v2.80 MR2	The `delete` field was added. The `download` field was changed to `export`.
FortiOS v2.80 MR3	Fields were removed from the `execute vpn certificate local` field and replaced with variables.
FortiOS v3.0 MR1	Removed all fields but `generate`.

FortiOS v3.0 MR3	Added fields `import, export`.
FortiOS v3.0 MR4	Added fields `auto, tftp` and variables `<ca_server_url>, <ca_identifier_str>` as result of the addition of the PKI certificate authentication feature.

Related topics

- execute vpn certificate local
- execute vpn certificate remote
- execute vpn certificate crl
- execute vpn sslvpn del-tunnel
- execute vpn sslvpn del-web
- vpn certificate ca
- vpn certificate local
- vpn certificate crl
- vpn certificate remote

vpn certificate crl

Use this command to get a CRL via LDAP, HTTP, or SCEP protocol, depending on the auto-update configuration.

In order to use the command execute vpn certificate crl, the authentication servers must already be configured.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The CA certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

Note: VPN peers must use digital certificates that adhere to the X.509 standard.

Note: Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

```
execute vpn certificate crl import auto <crl-name>
```

Variable	Description
`import`	Import the CRL from the configured LDAP, HTTP, or SCEP authentication server to the FortiGate unit.
`<crl-name>`	Enter the name of the CRL.
`auto`	Trigger an auto-update of the CRL from the configured LDAP, HTTP, or SCEP authentication server.

History

FortiOS v3.0 MR4 New.

Related topics

- execute vpn certificate ca
- execute vpn certificate local
- execute vpn certificate remote
- execute vpn sslvpn del-tunnel
- execute vpn sslvpn del-web
- vpn certificate ca
- vpn certificate local
- vpn certificate crl
- vpn certificate remote

vpn certificate local

Use this command to generate a local certificate, to export a local certificate from the FortiGate unit to a TFTP server, and to import a local certificate from a TFTP server to the FortiGate unit.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The local certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

When you generate a certificate request, you create a private and public key pair for the local FortiGate unit. The public key accompanies the certificate request. The private key remains confidential.

When you receive the signed certificate from the CA, use the `vpn certificate local` command to install it on the FortiGate unit.

Note: VPN peers must use digital certificates that adhere to the X.509 standard.

Note: Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax - `generate`

```
execute vpn certificate local generate <certificate-name_str> <key-length>
   {<host_ip> | <domain-name_str> | email-addr_str>}
   [<optional_information>]
```

Variable	Description
`<certificate-name_str>`	Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
`<host_ip>`	
`{<host_ip> | <domain-name_str> | email-addr_str>}`	Enter the host IP address (`host_ip`), the domain name (`domain-name_str`), or an email address (`email-addr_str`) to identify the FortiGate unit being certified. Preferably use an IP address or domain name. If this is impossible (such as with a dialup client), use an e-mail address. For `host_ip`, enter the IP address of the FortiGate unit. For `domain-name_str`, enter the fully qualified domain name of the FortiGate unit. For `email-addr_str`, enter an email address that identifies the FortiGate unit. If you specify a host IP or domain name, use the IP address or domain name associated with the interface on which IKE negotiations will take place (usually the external interface of the local FortiGate unit). If the IP address in the certificate does not match the IP address of this interface (or if the domain name in the certificate does not match a DNS query of the FortiGate unit's IP), then some implementations of IKE may reject the connection. Enforcement of this rule varies for different IPSec products.
`<key-length>`	Enter 1024, 1536 or 2048 for the size in bits of the encryption key.
`[<optional_information>]`	Enter `optional_information` as required to further identify the certificate. See "Optional information variables" on page 755 for the list of optional information variables. You must enter the optional variables in order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list. For example, to enter the `organization_name_str`, you must first enter the `country_code_str`, `state_name_str`, and `city_name_str`. While entering optional variables, you can type ? for help on the next required variable.

Optional information variables

Variable	Description
<country_code_str>	Enter the two-character country code. Enter `execute vpn certificates local generate <name_str> country` followed by a ? for a list of country codes. The country code is case sensitive. Enter `null` if you do not want to specify a country.
<state_name_str>	Enter the name of the state or province where the FortiGate unit is located.
<city_name_str>	Enter the name of the city, or town, where the person or organization certifying the FortiGate unit resides.
<organization-name_str>	Enter the name of the organization that is requesting the certificate for the FortiGate unit.
<organization-unit_name_str>	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiGate unit.
<email_address_str>	Enter a contact e-mail address for the FortiGate unit.
<ca_server_url>	Enter the URL of the CA (SCEP) certificate server that allows auto-signing of the request.
<challenge_password>	Enter the challenge password for the SCEP certificate server.

Example - `generate`

Use the following command to generate a local certificate request with the name `branch_cert`, the domain name `www.example.com` and a key size of `1536`.

```
execute vpn certificate local generate branch_cert 1536 www.example.com
```

Syntax - `import/export`

```
execute vpn certificate local import tftp <file-name_str> <tftp_ip>
execute vpn certificate local export tftp <certificate-name_str>
   <file-name_str> <tftp_ip>
```

Variable	Description
import	Import the local certificate from a TFTP server to the FortiGate unit.
export	Export or copy the local certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
<certificate-name_str>	Enter the name of the local certificate.
<tftp_ip>	Enter the TFTP server address.
<file-name_str>	Enter the file name on the TFTP server.
list	List local certificates.

Examples - `import/export`

Use the following command to export the local certificate request generated in the above example from the FortiGate unit to a TFTP server. The example uses the file name `testcert` for the downloaded file and the TFTP server address 192.168.21.54.

```
exec vpn certificate local export branch_cert testcert 192.168.21.54
```

Use the following command to import the signed local certificate named `branch_cert` to the FortiGate unit from a TFTP server with the address 192.168.21.54.

```
exec vpn certificate local import branch_cert 192.168.21.54
```

History

FortiOS v2.80 MR2	The `delete` field was added. The `download` field was changed to `export`.
FortiOS v2.80 MR3	Fields were removed from the `execute vpn certificate local` field and replaced with variables.
FortiOS v3.0 MR1	Removed all fields but generate.
FortiOS v3.0 MR3	Added fields `import, export`.
FortiOS v3.0 MR4	Added optional variables for certificate-based user authentication.

Related topics

- execute vpn certificate ca
- execute vpn certificate remote
- execute vpn certificate crl
- execute vpn sslvpn del-tunnel
- execute vpn sslvpn del-web
- vpn certificate ca
- vpn certificate local
- vpn certificate crl
- vpn certificate remote

vpn certificate remote

Use this command to import a remote certificate from a TFTP server, or export a remote certificate from the FortiGate unit to a TFTP server. The remote certificates are public certificates without a private key. They are used as OCSP (Online Certificate Status Protocol) server certificates.

Syntax

```
execute vpn certificate remote import tftp <file-name_str> <tftp_ip>
execute vpn certificate remote export tftp <certificate-name_str>
    <file-name_str> <tftp_ip>
```

Field/variable	Description
import	Import the remote certificate from the TFTP server to the FortiGate unit.
export	Export or copy the remote certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates.
<certificate-name_str>	Enter the name of the public certificate.
<file-name_str>	Enter the file name on the TFTP server.
<tftp_ip>	Enter the TFTP server address.
tftp	Import/export the remote certificate via a TFTP server.

History

FortiOS v3.0 MR4 New.

Related topics

- execute vpn certificate ca
- execute vpn certificate local
- execute vpn certificate crl
- execute vpn sslvpn del-tunnel
- execute vpn sslvpn del-web
- vpn certificate ca
- vpn certificate local
- vpn certificate crl
- vpn certificate remote

vpn sslvpn del-all

Use this command to delete all SSL VPN connections in this VDOM.

Syntax

```
execute vpn sslvpn del-all
```

History

FortiOS v4.0 MR1 New.

Related topics

- execute vpn sslvpn del-tunnel
- execute vpn sslvpn del-web

vpn sslvpn del-tunnel

Use this command to delete an SSL tunnel connection.

Syntax

```
execute vpn sslvpn del-tunnel <tunnel_index>
```

`<tunnel_index>` identifies which tunnel to delete if there is more than one active tunnel.

History

FortiOS v3.0	New.
FortiOS v3.0 MR1	Added `<tunnel_index>`.

Related topics

- vpn ssl settings

vpn sslvpn del-web

Use this command to delete an active SSL VPN web connection.

Syntax

```
execute vpn sslvpn del-web <web_index>
```

<web_index> identifies which web connection to delete if there is more than one active connection.

History

FortiOS v3.0 MR5 New.

Related topics

- vpn ssl settings

vpn sslvpn list

Use this command to list current SSL VPN tunnel connections.

Syntax

```
execute vpn sslvpn list {web | tunnel}
```

History

FortiOS v4.0 MR1 New.

Related topics

- execute vpn sslvpn del-tunnel
- execute vpn sslvpn del-web
- execute vpn sslvpn del-all

wireless-controller delete-wtp-image

Use this command to delete all firmware images for WLAN Termination Points (WTPs), also known as physical access points.

Syntax

```
execute wireless-controller delete-wtp-image
```

History

FortiOS v4.0 MR1 New.

Related topics

- execute wireless-controller upload-wtp-image

wireless-controller reset-wtp

Use this command to reset a physical access point (WTP).

Syntax

```
execute wireless-controller reset-wtp {<serialNumber_str> | all}
```

where `<serialNumber_str>` is the FortiWiFi unit serial number.

Use the `all` option to reset all APs.

History

FortiOS v4.0 MR1 New.

Related topics

- wireless-controller wtp

wireless-controller restart-daemon

Use this command to restart the wireless-controller feature.

Syntax

```
execute wireless-controller restart-daemon
```

History

FortiOS v4.0 MR1 New.

Related topics

- execute wireless-controller reset-wtp

wireless-controller upload-wtp-image

Use this command to upload a FortiWiFi firmware image to the FortiGate unit. Wireless APs controlled by this wireless controller can download the image as needed.

Syntax

FTP:

```
execute wireless-controller upload-wtp-image ftp <filename_str>
   <server_ipv4[:port_int]> [<username_str> <password_str>]
```

TFTP:

```
execute wireless-controller upload-wtp-image tftp <filename_str>
   <server_ipv4>
```

History

FortiOS v4.0 MR1 New.

Related topics

- execute wireless-controller delete-wtp-image

get

The get commands retrieve information about the operation and performance of your FortiGate unit.

This chapter contains the following sections:

endpoint-control app-detect predefined-category status

Use this command to retrieve information about predefined application detection signatures for Endpoint NAC.

Syntax

```
get endpoint-control app-detect predefined-category status
```

Example output (partial)

```
FG200A2907500558 # get endpoint-control app-detect predefined-category status
name: "Anti-Malware Software"
id: 1
group: 1

name: "Authentication and Authorization"
id: 2
group: 1

name: "Encryption, PKI"
id: 3
group: 1

name: "Firewalls"
id: 4
group: 1
```

Related topics

- config endpoint-control apps-detect rule-list rule-list

History

FortiOS v4.0 MR1 New.

endpoint-control app-detect predefined-group status

Use this command to retrieve information about predefined application detection groups for Endpoint NAC.

Syntax

```
get endpoint-control app-detect predefined-group status
```

Example output (partial)

```
FG200A2907500558 # get endpoint-control app-detect predefined-group status
name: "Security"
id: 1

name: "Multimedia"
id: 2

name: "Communication"
id: 3

name: "Critical Functions"
id: 4
```

Related topics

- config endpoint-control apps-detect rule-list

History

FortiOS v4.0 MR1 New.

endpoint-control app-detect predefined-signature status

Use this command to retrieve information about predefined application detection signatures for Endpoint NAC.

Syntax

```
get endpoint-control app-detect predefined-signature status
```

Example output (partial)

```
FG200A2907500558 # get endpoint-control app-detect predefined-signature status
name: "Apache HTTP Server"
id: 256
category: 26
vendor: 149

name: "RealPlayer (32-bit)"
id: 1
category: 10
vendor: 68

name: "VisualSVN Server"
id: 257
category: 26
vendor: 162

name: "QQ2009"
id: 2
category: 14
vendor: 78
```

Related topics

- config endpoint-control apps-detect rule-list rule-list

History

FortiOS v4.0 MR1 New.

endpoint-control app-detect predefined-vendor status

Use this command to retrieve information about predefined application detection vendors for Endpoint NAC.

Syntax

```
get endpoint-control app-detect predefined-vendor status
```

Example output (partial)

```
FG200A2907500558 # get endpoint-control app-detect predefined-vendor status
name: "Access Remote PC (www.access-remote-pc.com)"
id: 3

name: "ACD Systems, Ltd."
id: 4

name: "Adobe Systems Incorporated"
id: 5

name: "Alen Soft"
id: 6
```

Related topics

- config endpoint-control apps-detect rule-list rule-list

History

FortiOS v4.0 MR1 New.

firewall service predefined

Use this command to retrieve information about predefined services. If you do not specify a <service_name>, a long list will be displayed linking services to protocols.

The following information is available:

- destination port
- source port
- ICMP code
- ICMP type
- protocol
- protocol-number

Syntax

```
get firewall service predefined <service_name>
```

Example output

```
Fortigate-200A # get firewall service predefined FTP
name                : FTP
icmpcode            :
icmptype            :
protocol            : TCP/UDP
protocol-number     : 6
tcpport-range       : 21-21:0-65535
udpport-range       :

Fortigate-200A # get firewall service predefined SIP
name                : SIP
icmpcode            :
icmptype            :
protocol            : TCP/UDP
protocol-number     : 17
tcpport-range       :
udpport-range       : 5060-5060:0-65535

Fortigate-200A # get firewall service predefined AOL
name                : AOL
icmpcode            :
icmptype            :
protocol            : TCP/UDP
protocol-number     : 6
tcpport-range       : 5190-5194:0-65535
udpport-range       :
```

gui console status

Display information about the CLI console.

Syntax

```
get gui console status
```

Example

The output looks like this:

```
Preferences:
        User: admin
                Colour scheme (RGB): text=FFFFFF, background=000000
                Font: style=monospace, size=10pt
                History buffer=50 lines, external input=disabled
```

Related topics

- get gui topology status

History

FortiOS v3.0 MR5 New.

gui topology status

Display information about the topology viewer database. The topology viewer is available only if the Topology widget has been added to a customized web-based manager menu layout.

Syntax

```
get gui topology status
```

Example

The output looks like this:

```
Preferences:
        Canvas dimensions (pixels): width=780, height=800
        Colour scheme (RGB): canvas=12ff08, lines=bf0f00, exterior=ddeeee
        Background image: type=none, placement: x=0, y=0
        Line style: thickness=2

Custom background image file: none

Topology element database:
        __FortiGate__: x=260, y=340
        Office: x=22, y=105
        ISPnet: x=222, y=129
        __Text__: x=77, y=112: "Ottawa"
        __Text__: x=276, y=139: "Internet"
```

Related topics

- get gui console status

History

FortiOS v3.0 MR5 New.

hardware status

Report information about the FortiGate unit hardware.

Syntax

```
get hardware status
```

Example

The output looks like this:

```
FG600B3908600705 # get hardware status
Model name: Fortigate-620B
ASIC version: CP6
ASIC SRAM: 64M
CPU: Intel(R) Core(TM)2 Duo CPU     E4300  @ 1.80GHz
RAM: 2020 MB
Compact Flash: 493 MB /dev/sda
Hard disk: 76618 MB /dev/sdb
USB Flash: not available
Network Card chipset: Broadcom 570x Tigon3 Ethernet Adapter (rev.0x5784100)
```

History

FortiOS v3.0 MR2 New.

Related topics

- get system status

ips decoder status

Displays all the port settings of all the IPS decoders.

Syntax

```
get ips decoder status
```

The command output looks like this (partial output):

```
# get ips decoder status
decoder-name: "back_orifice"

decoder-name: "dns_decoder"
port_list: 53

decoder-name: "ftp_decoder"
port_list: 21

decoder-name: "http_decoder"

decoder-name: "im_decoder"

decoder-name: "imap_decoder"
port_list: 143
```

Ports are shown only for decoders with configurable port settings.

History

FortiOS v3.0 MR6 New command.

Related topics

- ips decoder
- get ips rule status

ips rule status

Displays current configuration information about IPS rules.

Syntax

```
get ips rule status
```

The output looks like this (partial output):

```
# get ips rule status
rule-name: "IP.Land"
rule-id: 12588
rev: 2.464
action: pass
status: disable
log: enable
log-packet: disable
severity: 3.high
service: All
location: server, client
os: All
application: All

rule-name: "IP.Loose.Src.Record.Route.Option"
rule-id: 12805
rev: 2.464
action: pass
status: disable
log: enable
log-packet: disable
severity: 2.medium
service: All
location: server, client
os: All
application: All
```

History

FortiOS v3.0 MR6 New command.

Related topics

- ips decoder
- get ips decoder status
- ips rule

ipsec tunnel list

List the current IPSec VPN tunnels and their status.

Syntax

```
get ipsec tunnel list
```

Example

The output looks like this:

```
NAME    REMOTE-GW        PROXY-ID-SOURCE         PROXY-ID-DESTINATION  STATUS
TIMEOUT
VPN1    172.20.120.5:500 0.0.0.0/255.255.255.255 172.20.120.5/172.20.120.5 up
1786
```

NAME	The name of the configured tunnel.
REMOTE-GW	The public IP address and UDP port of the remote host device, or if a NAT device exists in front of the remote host, the public IP address and UDP port of the NAT device.
PROXY- ID-SOURCE	The IP address range of the hosts, servers, or private networks behind the FortiGate unit that are available through the VPN tunnel.
PROXY- ID-DESTINATION	This field displays IP addresses as a range. When a FortiClient dialup client establishes a tunnel: • If VIP addresses are not used, the Proxy ID Destination field displays the public IP address of the remote host Network Interface Card (NIC). • If VIP addresses were configured (manually or through FortiGate DHCP relay), the Proxy ID Destination field displays either the VIP address belonging to the FortiClient dialup client, or the subnet address from which VIP addresses were assigned. When a FortiGate dialup client establishes a tunnel, the Proxy ID Destination field displays the IP address of the remote private network.
STATUS	Tunnel status: up or down.
TIMEOUT	The number of seconds before the next phase 2 key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife duration setting. When the phase 2 key expires, a new key is generated without interrupting service.

History

FortiOS v3.0 MR2 New.

Related topics

- vpn ipsec phase1
- vpn ipsec phase1-interface
- vpn ipsec manualkey
- vpn ipsec manualkey-interface

report database schema

Use this command to display the SQL report database schema. For more information, see “SQL reports database schema” on page 268.

Syntax

```
get report database schema
```

History

FortiOS 4.0 MR1 New.

router info bfd neighbor

Use this command to list state information about the neighbors in the bi-directional forwarding table.

Syntax

```
get router info bfd neighbour
```

History

FortiOS v3.0 MR4 New.

router info bgp

Use this command to display information about the BGP configuration.

Syntax

```
get router info bgp <keyword>
```

<keyword>	Description
cidr-only	Show all BGP routes having non-natural network masks.
community	Show all BGP routes having their COMMUNITY attribute set.
community-info	Show general information about the configured BGP communities, including the routes in each community and their associated network addresses.
community-list	Show all routes belonging to configured BGP community lists.
dampening {dampened-paths | flap-statistics | parameters}	Display information about dampening: • Type dampened-paths to show all paths that have been suppressed due to flapping. • Type flap-statistics to show flap statistics related to BGP routes. • Type parameters to show the current dampening settings.
filter-list	Show all routes matching configured AS-path lists.
inconsistent-as	Show all routes associated with inconsistent autonomous systems of origin.
memory	Show the BGP memory table.
neighbors [<address_ipv4> | <address_ipv4> advertised-routes | <address_ipv4> received prefix-filter | <address_ipv4> received-routes | <address_ipv4> routes]	Show information about connections to TCP and BGP neighbors.
network [<address_ipv4mask>]	Show general information about the configured BGP networks, including their network addresses and associated prefixes.
network-longer-prefixes <address_ipv4mask>	Show general information about the BGP route that you specify (for example, 12.0.0.0/14) and any specific routes associated with the prefix.
paths	Show general information about BGP AS paths, including their associated network addresses.
prefix-list <name>	Show all routes matching configured prefix list <name>.
quote-regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730$) and enable the use of output modifiers (for example, include, exclude, and begin) to search the results.
regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730$).
route-map	Show all routes matching configured route maps.
scan	Show information about next-hop route scanning, including the scan interval setting.
summary	Show information about BGP neighbor status.

Example

For the command `get router info bgp memory`, the output looks like:

```
Memory type                          Alloc count   Alloc bytes
==================================== ============= ===============
BGP structure                      :           2            1408
BGP VR structure                   :           2             104
BGP global structure               :           1              56
BGP peer                           :           2            3440
BGP as list master                 :           1              24
Community list handler             :           1              32
BGP Damp Reuse List Array          :           2            4096
BGP table                          :          62             248
---------------------------------- ------------- ---------------
Temporary memory                   :        4223           96095
Hash                               :           7             140
Hash index                         :           7           28672
Hash bucket                        :          11             132
Thread master                      :           1             564
Thread                             :           4             144
Link list                          :          32             636
Link list node                     :          24             288
Show                               :           1             396
Show page                          :           1            4108
Show server                        :           1              36
Prefix IPv4                        :          10              80
Route table                        :           4              32
Route node                         :          63            2772
Vector                             :        2180           26160
Vector index                       :        2180           18284
Host config                        :           1               2
Message of The Day                 :           1             100
IMI Client                         :           1             708
VTY master                         :           1              20
VTY if                             :          11            2640
VTY connected                      :           5             140
Message handler                    :           2             120
NSM Client Handler                 :           1           12428
NSM Client                         :           1            1268
Host                               :           1              64
Log information                    :           2              72
Context                            :           1             232
---------------------------------- ------------- ---------------
bgp proto specifc allocations :         9408 B
bgp generic allocations       :       196333 B
bgp total allocations         :       205741 B
```

History

FortiOS v3.0 New.

FortiOS v3.0 MR2 Command moved from ‘router’ to ‘get’ chapter.

Related topics

- router aspath-list
- router bgp
- router community-list

router info multicast

Use this command to display information about a Protocol Independent Multicasting (PIM) configuration. Multicast routing is supported in the root virtual domain only.

Syntax

```
get router info multicast <keywords>
```

<keywords>	Description
igmp	Show Internet Group Management Protocol (IGMP) membership information according to one of these qualifiers: • Type `groups [{<interface-name> | <group-address>}]` to show IGMP information for the multicast group(s) associated with the specified interface or multicast group address. • Type `groups-detail [{<interface-name> | <group-address>}]` to show detailed IGMP information for the multicast group(s) associated with the specified interface or multicast group address. • Type `interface [<interface-name>]` to show IGMP information for all multicast groups associated with the specified interface.
pim dense-mode	Show information related to dense mode operation according to one of these qualifiers: • Type `interface` to show information about PIM-enabled interfaces. • Type `interface-detail` to show detailed information about PIM-enabled interfaces. • Type `neighbor` to show the current status of PIM neighbors. • Type `neighbor-detail` to show detailed information about PIM neighbors. • Type `next-hop` to show information about next-hop PIM routers. • Type `table [<group-address>][<source-address>]` to show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.
pim sparse-mode	Show information related to sparse mode operation according to one of these qualifiers: • Type `bsr-info` to show Boot Strap Router (BSR) information. • Type `interface` to show information about PIM-enabled interfaces. • Type `interface-detail` to show detailed information about PIM-enabled interfaces. • Type `neighbor` to show the current status of PIM neighbors. • Type `neighbor-detail` to show detailed information about PIM neighbors. • Type `next-hop` to show information about next-hop PIM routers. • Type `rp-mapping` to show Rendezvous Point (RP) information. • Type `table [<group-address>][<source-address>]` to show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.
table [<group-address>] [<source-address>]	Show the multicast routing table entries associated with the specified multicast group address and/or multicast source address.
table-count [<group-address>] [<source-address>]	Show statistics related to the specified multicast group address and/or multicast source address.

Examples

This example displays all of the PIM entries in the multicast routing table:

```
get router info multicast table
```

This example displays IGMP information for the multicast group associated with multicast group address 239.254.2.0:

```
get router info multicast igmp groups 239.254.2.0
```

History

FortiOS v3.0	New.
FortiOS v3.0 MR2	Moved from ‘router’ to ‘get’ chapter.

Related topics

- router multicast
- execute modem trigger

router info ospf

Use this command to display information about the FortiGate OSPF configuration and/or the Link-State Advertisements (LSAs) that the FortiGate unit obtains and generates. An LSA identifies the interfaces of all OSPF-enabled routers in an area, and provides information that enables OSPF-enabled routers to select the shortest path to a destination.

Syntax

```
get router info ospf <keyword>
```

<keyword>		Description
border-routers		Show OSPF routing table entries that have an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) as a destination.
database <qualifier>		Show information from the OSPF routing database according to one of these qualifiers. target can be one of the following values: • Type adv_router <address_ipv4> to limit the information to LSAs originating from the router at the specified IP address. • Type self-originate <address_ipv4> to limit the information to LSAs originating from the FortiGate unit.
	adv-router <address_ipv4>	Type adv-router <address_ipv4> to show ospf Advertising Router link states for the router at the given IP address.
	asbr-summary <target>	Type asbr-summary to show information about ASBR summary LSAs.
	brief	Type brief to show the number and type of LSAs associated with each OSPF area.
	external <target>	Type external to show information about external LSAs.
	max-age	Type max-age to show all LSAs in the MaxAge list.
	network <target>	Type network to show information about network LSAs.
	nssa-external <target>	Type nssa-external to show information about not-so-stubby external LSAs.
	opaque-area <address_ipv4>	Type opaque-area <address_ipv4> to show information about opaque Type 10 (area-local) LSAs (see RFC 2370).
	opaque-as <address_ipv4>	Type opaque-as <address_ipv4> to show information about opaque Type 11 LSAs (see RFC 2370), which are flooded throughout the AS.
	opaque-link <address_ipv4>	Type opaque-link <address_ipv4> to show information about opaque Type 9 (link-local) LSAs (see RFC 2370).
	router <target>	Type router to show information about router LSAs.
	self-originate	Type self-originate to show self-originated LSAs.
	summary <target>	Type summary to show information about summary LSAs.
interface [<interface_name>]		Show the status of one or all FortiGate interfaces and whether OSPF is enabled on those interfaces.

<keyword>	Description
neighbor [all | <neighbor_id> | detail | detail all | interface <address_ipv4>]	Show general information about OSPF neighbors, excluding down-status neighbors: • Type all to show information about all neighbors, including down-status neighbors. • Type <neighbor_id> to show detailed information about the specified neighbor only. • Type detail to show detailed information about all neighbors, excluding down-status neighbors. • Type detail all to show detailed information about all neighbors, including down-status neighbors. • Type interface <address_ipv4> to show neighbor information based on the FortiGate interface IP address that was used to establish the neighbor's relationship.
route	Show the OSPF routing table.
status	Show general information about the OSPF routing processes.
virtual-links	Show information about OSPF virtual links.

Examples

The following example shows how to display information from LSAs originating from a neighboring router at IP address 10.2.4.1:

```
get router info ospf database router adv_router 10.2.4.1
```

The following example shows how to display the number and type of LSAs associated with each OSPF area to which the FortiGate unit is linked:

```
get router info ospf database brief
```

The following command shows the status of all FortiGate interfaces and whether OSPF is enabled on those interfaces.

```
get router info ospf interface
```

History

FortiOS v2.80 MR1	New.
FortiOS v2.80 MR2	Renamed from execute router show ospf.
FortiOS v2.80 MR7	Added status keyword.
FortiOS v3.0	Added variants of the database and neighbor keywords.
FortiOS v3.0 MR1	No change.
FortiOS v3.0 MR2	Moved from 'router' to 'get' chapter.

Related topics

- execute router restart
- get router info protocols
- get router info routing-table
- system interface
- router ospf

router info protocols

Use this command to show the current states of active routing protocols. Inactive protocols are not displayed.

Syntax

```
get router info protocols
```

```
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
  Routing for Networks:
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Distance: (default is 120)

Routing Protocol is "ospf 0"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing:
  Routing for Networks:
  Routing Information Sources: Gateway         Distance      Last Update
  Distance: (default is 110) Address         Mask            Distance List

Routing Protocol is "bgp 5"
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Default local-preference applied to incoming route is 100
  Redistributing:
  Neighbor(s):
  Address AddressFamily FiltIn FiltOut DistIn DistOut RouteMapIn RouteMapOut
Weight
  192.168.20.10 unicast
```

History

FortiOS v2.80	New.
FortiOS v2.80 MR2	Renamed from `execute router show protocols`.
FortiOS v3.0 MR2	Moved from ‘router’ to ‘get’ chapter.

Related topics

- execute router restart
- get router info rip, get router info routing-table
- router rip, router ospf

router info rip

Use this command to display information about the RIP configuration.

Syntax

```
get router info rip <keyword>
```

<keyword>	Description
database	Show the entries in the RIP routing database.
interface [<interface_name>]	Show the status of the specified FortiGate unit interface <interface_name> and whether RIP is enabled. If interface is used alone it lists all the FortiGate unit interfaces and whether RIP is enabled on each.

Example

The following command displays the RIP configuration information for the port1 interface:

```
get router info rip interface port1
```

History

FortiOS v2.80	New.
FortiOS v2.80 MR2	Renamed from `execute router show rip`.
FortiOS v3.0	Added optional `interface_name` component to `interface` attribute.
FortiOS v3.0 MR1	No change.
FortiOS v3.0 MR2	Move from ‘router’ to ‘get’ chapter.

Related topics

- get router info protocols
- get router info routing-table
- router rip
- system interface

router info routing-table

Use this command to display the routes in the routing table.

Syntax

```
get router info routing-table <keyword>
```

<keyword>	Description
all	Show all entries in the routing table.
bgp	Show the BGP routes in the routing table.
connected	Show the connected routes in the routing table.
database	Show the routing information database.
details [<address_ipv4mask>]	Show detailed information about a route in the routing table, including the next-hop routers, metrics, outgoing interfaces, and protocol-specific information.
ospf	Show the OSPF routes in the routing table.
rip	Show the RIP routes in the routing table.
static	Show the static routes in the routing table.

Example

The following command displays the entire routing table:

```
get router info routing-table all
```

History

FortiOS v2.80	New.
FortiOS v2.80 MR2	Renamed from `execute router show routing_table`.
FortiOS v3.0	Added <keyword> variable to command syntax and replaced underscore character in command with hyphen.
FortiOS v3.0 MR1	Added `database keyword`.
FortiOS v3.0 MR2	Moved from 'router' to 'get' chapter.

Related topics

- execute router restart
- get router info ospf
- get router info protocols
- get router info rip
- router policy
- router rip
- router static
- router static6
- system interface

router info6 bgp

Use this command to display information about the BGP IPv6 configuration.

Syntax

```
get router info6 bgp <keyword>
```

<keyword>	Description
community	Show all BGP routes having their COMMUNITY attribute set.
community-list	Show all routes belonging to configured BGP community lists.
dampening {dampened-paths | flap-statistics | parameters}	Display information about dampening: • Type dampened-paths to show all paths that have been suppressed due to flapping. • Type flap-statistics to show flap statistics related to BGP routes. • Type parameters to show the current dampening settings.
filter-list	Show all routes matching configured AS-path lists.
inconsistent-as	Show all routes associated with inconsistent autonomous systems of origin.
neighbors [<address_ipv6mask>	Show information about connections to TCP and BGP neighbors.
network [<address_ipv6mask>]	Show general information about the configured BGP networks, including their network addresses and associated prefixes.
network-longer-prefixes <address_ipv6mask>	Show general information about the BGP route that you specify (for example, 12.0.0.0/14) and any specific routes associated with the prefix.
paths	Show general information about BGP AS paths, including their associated network addresses.
prefix-list <name>	Show all routes matching configured prefix list <name>.
quote-regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730$) and enable the use of output modifiers (for example, include, exclude, and begin) to search the results.
regexp <regexp_str>	Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730$).
route-map	Show all routes matching configured route maps.
summary	Show information about BGP neighbor status.

History

FortiOS v4.0 MR1 New.

router info6 interface

Use this command to display information about IPv6 interfaces.

Syntax

```
get router info6 interface <interface_name>
```

The command returns the status of the interface and the assigned IPv6 address.

```
dmz2                      [administratively down/down]
    2001:db8:85a3:8d3:1319:8a2e:370:7348
    fe80::209:fff:fe04:4cfd
```

History

FortiOS v4.0 New.

router info6 ospf

Use this command to display information about the OSPF IPv6 configuration.

Syntax

```
get router info6 ospf
```

History

FortiOS v4.0 MR1 New.

router info6 protocols

Use this command to display information about the configuration of all IPv6 dynamic routing protocols.

Syntax

```
get router info6 protocols
```

History

FortiOS v4.0 MR1 New.

router info6 rip

Use this command to display information about the RIPng configuration.

Syntax

```
get router info6 rip
```

History

FortiOS v4.0 MR1 New.

router info6 routing-table

Use this command to display the routes in the IPv6 routing table.

Syntax

```
get router info6 routing-table <item>
```

where <item> is one of the following:

Variable	Description
`<ipv6_ip>`	Destination IPv6 address or prefix.
`bgp`	Show BGP routing table entries.
`connected`	Show connected routing table entries.
`database`	Show routing information base.
`ospf`	Show OSPF routing table entries.
`rip`	Show RIP routing table entries.
`static`	Show static routing table entries.

History

FortiOS v4.0 New.

system admin list

View a list of all the current administration sessions.

Syntax

```
get system admin list
```

Example

The output looks like this:

```
# get system admin list
username local  device                    remote                 started
admin    sshv2  port1:172.20.120.148:22  172.20.120.16:4167   2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443 172.20.120.161:56365 2006-08-09 12:24:20
admin    https  port1:172.20.120.148:443 172.20.120.16:4214   2006-08-09 12:25:29
```

username	Name of the admin account for this session
local	The protocol this session used to connect to the FortiGate unit.
device	The interface, IP address, and port used by this session to connect to the FortiGate unit.
remote	The IP address and port used by the originating computer to connect to the FortiGate unit.
started	The time the current session started.

History

FortiOS v3.0 MR3 New command.

system admin status

View the status of the currently logged in admin and their session.

Syntax

```
get system admin status
```

Example

The output looks like this:

```
# get system admin status
username: admin
login local: sshv2
login device: port1:172.20.120.148:22
login remote: 172.20.120.16:4167
login vdom: root
login started: 2006-08-09 12:24:20
current time: 2006-08-09 12:32:12
```

`username`	Name of the admin account currently logged in.
`login local`	The protocol used to start the current session.
`login device`	The login information from the FortiGate unit including interface, IP address, and port number.
`login remote`	The computer the user is logging in from including the IP address and port number.
`login vdom`	The virtual domain the admin is current logged into.
`login started`	The time the current session started.
`current time`	The current time of day on the FortiGate unit

History

FortiOS v3.0 MR3 New command.

system arp

View the ARP table entries on the FortiGate unit.

This command is not available in multiple VDOM mode.

Syntax

```
get system arp
```

Example

The output looks like this:

```
# get system arp
Address           Age(min)   Hardware Addr      Interface
172.20.120.16     0          00:0d:87:5c:ab:65 internal
172.20.120.138    0          00:08:9b:09:bb:01 internal
```

Address	The IP address that is linked to the MAC address.
Age	Current duration of the ARP entry in minutes.
Hardware Addr	The hardware, or MAC address, to link with this IP address.
Interface	The physical interface the address is on.

History

FortiOS v3.0 New.

FortiOS v3.0 MR1 No change.

FortiOS v3.0 MR2 Moved from ‘system’ to ‘get’ chapter.

FortiOS v3.0 MR4 Output format changed.

Related topics

- system arp-table
- system proxy-arp

system central-management

View information about the Central Management System configuration.

Syntax

```
get system central-management
```

Example

The output looks like this:

```
FG600B3908600705 # get system central-management
status              : enable
type                : fortimanager
auto-backup         : disable
schedule-config-restore: enable
schedule-script-restore: enable
allow-push-configuration: enable
allow-pushd-firmware: enable
allow-remote-firmware-upgrade: enable
allow-monitor       : enable
fmg                 : 172.20.120.161
vdom                : root
authorized-manager-only: enable
serial-number       : "FMG-3K2404400063"
```

History

FortiOS v3.0 MR5 New.

FortiOS v4.0 Command name changed to `get system central-management`.

system checksum

View the checksums for global, root, and all.

Syntax

```
get system checksum status
```

Example

The output looks like this:

```
# get system checksum status
global: 7a 87 3c 14 93 bc 98 92 b0 58 16 f2 eb bf a4 15
root: bb a4 80 07 42 33 c2 ff f1 b5 6e fe e4 bb 45 fb
all: 1c 28 f1 06 fa 2e bc 1f ed bd 6b 21 f9 4b 12 88
```

History

FortiOS v3.0 MR4 New.

system cmdb status

View information about cmdbsvr on the FortiGate unit. FortiManager uses some of this information.

Syntax

```
get system cmdb status
```

Example

The output looks like this:

```
# get system cmdb status
version: 1
owner id: 18
update index: 6070
config checksum: 12879299049430971535
last request pid: 68
last request type: 29
last request: 78
```

`version`	Version of the cmdb software.
`owner id`	Process ID of the cmdbsvr daemon.
`update index`	The updated index shows how many changes have been made in cmdb.
`config checksum`	The config file version used by FortiManager.
`last request pid`	The last process to access the cmdb.
`last requst type`	Type of the last attempted access of cmdb.
`last request`	The number of the last attempted access of cmdb.

History

FortiOS v3.0 MR2 New command.

system dashboard

List the available dashboard widgets. The `help:` field explains widget purpose.

FortiManager uses this information.

Syntax

```
get system dashboard [<widget_name>]
```

Example

The output looks like this:

```
# get system dashboard
== [ sysinfo ]
name: sysinfo    help: system information
== [ licinfo ]
name: licinfo    help: license information
== [ sysop ]
name: sysop    help: system operation
== [ sysres ]
name: sysres    help: system resource
== [ alert ]
name: alert    help: alert console
== [ statistics ]
name: statistics    help: statistics
== [ jsconsole ]
name: jsconsole    help: CLI console
== [ sessions ]
name: sessions    help: top sessions
== [ top-viruses ]
name: top-viruses    help: top detected viruses
== [ top-attacks ]
name: top-attacks    help: top detected attacks
== [ tr-history ]
name: tr-history    help: traffic history
```

If you specify a specific widget, the output looks like this:

```
# get system dashboard sysinfo
name                : sysinfo
help                : system information
```

History

FortiOS v3.0 MR4 New command.

system fdp-fortianalyzer

Use this command to display the serial number of the FortiAnalyzer unit you use for logging.

Syntax

```
get system fdp-fortianalyzer
```

The result looks like this:

```
# get system fdp-fortianalyzer
SERIAL NUMBER
-------------
FL800B3908000420
```

History

FortiOS v4.0 New.

system fortianalyzer-connectivity

Display connection and remote disk usage information about a connected FortiAnalyzer unit.

Syntax

```
get fortianalyzer-connectivity status
```

Example

The output looks like this:

```
# get system fortianalyzer-connectivity status
Status: connected
Disk Usage: 0%
```

History

FortiOS v3.0 MR4 New command.

system fortiguard-log-service status

Command returns information about the status of the FortiGuard Log & Analysis Service including license and disk information.

Syntax

```
get system fortiguard-log-service status
```

Example

This shows a sample output.

```
# get system fortiguard-log-service status
FortiGuard Log & Analysis Service
Expire on: 20071231
Total disk quota: 1111 MB
Max daily volume: 111 MB
Current disk quota usage: n/a
```

History

FortiOS v3.0 MR4 New command.

system fortiguard-service status

COMMAND REPLACED. Command returns information about the status of the FortiGuard service including the name, version late update, method used for the last update and when the update expires. This information is shown for the AV Engine, virus definitions, attack definitions, and the IPS attack engine.

Syntax

```
get system fortiguard-service status
```

Example

This shows a sample output.

```
NAME                VERSION LAST UPDATE          METHOD    EXPIRE
AV Engine           2.002   2006-01-26 19:45:00  manual    2006-06-12 08:00:00
Virus Definitions   6.513   2006-06-02 22:01:00  manual    2006-06-12 08:00:00
Attack Definitions  2.299   2006-06-09 19:19:00  manual    2006-06-12 08:00:00
IPS Attack Engine   1.015   2006-05-09 23:29:00  manual    2006-06-12 08:00:00
```

History

FortiOS v3.0 MR2 New command.

FortiOS v3.0 MR5 Command replaced with `get system central-mgmt status`

system ha status

Use this command to display information about an HA cluster. The command displays general HA configuration settings. The command also displays information about how the cluster unit that you have logged into is operating in the cluster.

Usually you would log into the primary unit CLI using SSH or telnet. In this case the `get system ha status` command displays information about the primary unit first, and also displays the HA state of the primary unit (the primary unit operates in the work state). However, if you log into the primary unit and then use the `execute ha manage` command to log into a subordinate unit, (or if you use a console connection to log into a subordinate unit) the `get system status` command displays information about this subordinate unit first, and also displays the HA state of this subordinate unit. The state of a subordinate unit is work for an active-active cluster and standby for an active-passive cluster.

For a virtual cluster configuration, the `get system ha status` command displays information about how the cluster unit that you have logged into is operating in virtual cluster 1 and virtual cluster 2. For example, if you connect to the cluster unit that is the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2, the output of the `get system ha status` command shows virtual cluster 1 in the work state and virtual cluster 2 in the standby state. The `get system ha status` command also displays additional information about virtual cluster 1 and virtual cluster 2.

Syntax

```
get system ha status
```

The command display includes the following fields. For more information see the examples that follow.

`Model`	The FortiGate model number.
`Mode`	The HA mode of the cluster: a-a or a-p.
`Group`	The group ID of the cluster.
`Debug`	The debug status of the cluster.
`ses_pickup`	The status of session pickup: enable or disable.
`load_balance`	The status of the `load-balance-all` field: enable or disable. Displayed for active-active clusters only.
`schedule`	The active-active load balancing schedule. Displayed for active-active clusters only.
`Master` `Slave`	`Master` displays the device priority, host name, serial number, and actual cluster index of the primary (or master) unit. `Slave` displays the device priority, host name, serial number, and actual cluster index of the subordinate (or slave, or backup) unit or units. The list of cluster units changes depending on how you log into the CLI. Usually you would use SSH or telnet to log into the primary unit CLI. In this case the primary unit would be at the top the list followed by the other cluster units. If you use `execute ha manage` or a console connection to log into a subordinate unit CLI, and then enter `get system ha status` the subordinate unit that you have logged into appears at the top of the list of cluster units.
`number of vcluster`	The number of virtual clusters. If virtual domains are not enabled, the cluster has one virtual cluster. If virtual domains are enabled the cluster has two virtual clusters.

`vcluster 1`	The HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 1. If virtual domains are not enabled, `vcluster 1` displays information for the cluster. If virtual domains are enabled, `vcluster 1` displays information for virtual cluster 1. The HA heartbeat IP address is 10.0.0.1 if you are logged into a the primary unit of virtual cluster 1 and 10.0.0.2 if you are logged into a subordinate unit of virtual cluster 1. `vcluster 1` also lists the primary unit (master) and subordinate units (slave) in virtual cluster 1. The list includes the operating cluster index and serial number of each cluster unit in virtual cluster 1. The cluster unit that you have logged into is at the top of the list. If virtual domains are not enabled and you connect to the primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the primary unit. If virtual domains are not enabled and you connect to a subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you have logged into. If virtual domains are enabled and you connect to the virtual cluster 1 primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the virtual cluster 1 primary unit. If virtual domains are enabled and you connect to the virtual cluster 1 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you are logged into. In a cluster consisting of two cluster units operating without virtual domains enabled all clustering actually takes place in virtual cluster 1. HA is designed to work this way to support virtual clustering. If this cluster was operating with virtual domains enabled, adding virtual cluster 2 is similar to adding a new copy of virtual cluster 1. Virtual cluster 2 is visible in the `get system ha status` command output when you add virtual domains to virtual cluster 2.
`vcluster 2`	`vcluster 2` only appears if virtual domains are enabled. `vcluster 2` displays the HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 2. The HA heartbeat IP address is 10.0.0.2 if you are logged into the primary unit of virtual cluster 2 and 10.0.0.1 if you are logged into a subordinate unit of virtual cluster 2. `vcluster 2` also lists the primary unit (master) and subordinate units (slave) in virtual cluster 2. The list includes the cluster index and serial number of each cluster unit in virtual cluster 2. The cluster unit that you have logged into is at the top of the list. If you connect to the virtual cluster 2 primary unit CLI, the HA state of the cluster unit in virtual cluster 2 is `work`. The display lists the cluster units starting with the virtual cluster 2 primary unit. If you connect to the virtual cluster 2 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 2 is `standby`. The display lists the cluster units starting with the subordinate unit that you are logged into.

Examples

The following example shows `get system ha status` output for a cluster of two FortiGate-5001SX units operating in active-active mode. The cluster group ID, session pickup, load balance all, and the load balancing schedule are all set to the default values. The device priority of the primary unit is also set to the default value. The device priority of the subordinate unit has been reduced to 100. The host name of the primary unit is `5001_Slot_4`. The host name of the subordinate unit in is `5001_Slot_3`.

The command output was produced by connecting to the primary unit CLI (host name `5001_Slot_4`).

```
Model: 5000
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
load_balance: disable
schedule: round robin
Master:128 5001_Slot_4      FG50012204400045 1
Slave :100 5001_Slot_3      FG50012205400050 0
number of vcluster: 1
vcluster 1: work 10.0.0.2
```

```
Master:0 FG50012204400045
Slave :1 FG50012205400050
```

The following command output was produced by using `execute HA manage 0` to log into the subordinate unit CLI of the cluster shown in the previous example. The host name of the subordinate unit is `5001_Slot_3.`

```
Model: 5000
Mode: a-a
Group: 0
Debug: 0
ses_pickup: disable
load_balance: disable
schedule: round robin
Slave :100 5001_Slot_3      FG50012205400050 0
Master:128 5001_Slot_4      FG50012204400045 1
number of vcluster: 1
vcluster 1: work 10.0.0.2
Slave :1 FG50012205400050
Master:0 FG50012204400045
```

About the HA cluster index and the execute ha manage command

When a cluster starts up the FortiGate Cluster Protocol (FGCP) assigns a cluster index and a HA heartbeat IP address to each cluster unit based on the serial number of the cluster unit. The FGCP selects the cluster unit with the highest serial number to become the primary unit. The FGCP assigns a cluster index of 0 and an HA heartbeat IP address of 10.0.0.1 to this unit. The FGCP assigns a cluster index of 1 and an HA heartbeat IP address of 10.0.0.2 to the cluster unit with the second highest serial number. If the cluster contains more units, the cluster unit with the third highest serial number is assigned a cluster index of 2 and an HA heartbeat IP address of 10.0.0.3, and so on. You can display the cluster index assigned to each cluster unit using the `get system ha status` command. Also when you use the `execute ha manage` command you select a cluster unit to log into by entering its cluster index.

The cluster index and HA heartbeat IP address only change if a unit leaves the cluster or if a new unit joins the cluster. When one of these events happens, the FGCP resets the cluster index and HA heartbeat IP address of each cluster unit according to serial number in the same way as when the cluster first starts up.

Each cluster unit keeps its assigned cluster index and HA heartbeat IP address even as the units take on different roles in the cluster. After the initial cluster index and HA heartbeat IP addresses are set according to serial number, the FGCP checks other primary unit selection criteria such as device priority and monitored interfaces. Checking these criteria could result in selecting a cluster unit without the highest serial number to operate as the primary unit.

Even if the cluster unit without the highest serial number now becomes the primary unit, the cluster indexes and HA heartbeat IP addresses assigned to the individual cluster units do not change. Instead the FGCP assigns a second cluster index, which could be called the operating cluster index, to reflect this role change. The operating cluster index is 0 for the primary unit and 1 and higher for the other units in the cluster. By default both sets of cluster indexes are the same. But if primary unit selection selects the cluster unit that does not have the highest serial number to be the primary unit then this cluster unit is assigned an operating cluster index of 0. The operating cluster index is used by the FGCP only. You can display the operating cluster index assigned to each cluster unit using the `get system ha status` command. There are no CLI commands that reference the operating cluster index.

Note: Even though there are two cluster indexes there is only one HA heartbeat IP address and the HA heartbeat address is not affected by a change in the operating cluster index.

Using the execute ha manage command

When you use the CLI command `execute ha manage <index_integer>` to connect to the CLI of another cluster unit, the `<index_integer>` that you enter is the cluster index of the unit that you want to connect to.

Using get system ha status to display cluster indexes

You can display the cluster index assigned to each cluster unit using the CLI command `get system ha status`. The following example shows the information displayed by the `get system ha status` command for a cluster consisting of two FortiGate-5001SX units operating in active-passive HA mode with virtual domains not enabled and without virtual clustering.

```
get system ha status
Model: 5000
Mode: a-p
Group: 0
Debug: 0
ses_pickup: disable
Master:128 5001_slot_7 FG50012205400050 0
Slave :128 5001_slot_11 FG50012204400045 1
number of vcluster: 1
vcluster 1: work 10.0.0.1
Master:0 FG50012205400050
Slave :1 FG50012204400045
```

In this example, the cluster unit with serial number FG50012205400050 has the highest serial number and so has a cluster index of 0 and the cluster unit with serial number FG50012204400045 has a cluster index of 1. From the CLI of the primary (or master) unit of this cluster you can connect to the CLI of the subordinate (or slave) unit using the following command:

```
execute ha manage 1
```

This works because the cluster unit with serial number FG50012204400045 has a cluster index of 1.

The `get system ha status` command output shows two similar lists of indexes and serial numbers. The listing on the sixth and seventh lines of the command output are the cluster indexes assigned according to cluster unit serial number. These are the cluster indexes that you enter when using the `execute ha manage` command. The cluster indexes shown in the last two lines of the command output are the operating cluster indexes that reflect how the cluster units are actually operating in the cluster. In this example both sets of cluster indexes are the same.

The last three lines of the command output display the status of vcluster 1. In a cluster consisting of two cluster units operating without virtual domains enabled all clustering actually takes place in virtual cluster 1. HA is designed to work this way to support virtual clustering. If this cluster was operating with virtual domains enabled, adding virtual cluster 2 is similar to adding a new copy of virtual cluster 1. Virtual cluster 2 is visible in the `get system ha status` command output when you add virtual domains to virtual cluster 2.

The HA heartbeat IP address displayed on line 8 is the HA heartbeat IP address of the cluster unit that is actually operating as the primary unit. For a default configuration this IP address will always be 10.0.0.1 because the cluster unit with the highest serial number will be the primary unit. This IP address changes if the operating primary unit is not the primary unit with the highest serial number.

Example: actual and operating cluster indexes do not match

This example shows get system ha status command output for same cluster of two FortiGate-5001SX units. However, in this example the device priority of the cluster unit with the serial number FG50012204400045 is increased to 200. As a result the cluster unit with the lowest serial number becomes the primary unit. This means the actual and operating cluster indexes of the cluster units do not match.

```
get system ha status
Model: 5000
Mode: a-p
Group: 0
Debug: 0
ses_pickup: disable
Master:128 5001_slot_7 FG50012205400050 0
Slave :200 5001_slot_11 FG50012204400045 1
number of vcluster: 1
vcluster 1: work 10.0.0.2
Master:1 FG50012205400050
Slave :0 FG50012204400045
```

The actual cluster indexes have not changed but the operating cluster indexes have. Also, the HA heartbeat IP address displayed for vcluster 1 has changed to 10.0.0.2.

Virtual clustering example output

The `get system ha status` command output is the same if a cluster is operating with virtual clustering turned on but with all virtual domains in virtual cluster 1. The following `get system ha status` command output example shows the same cluster operating as a virtual cluster with virtual domains in virtual cluster 1 and added to virtual cluster 2. In this example the cluster unit with serial number FG50012204400045 is the primary unit for virtual cluster 1 and the cluster unit with serial number FG50012205400050 is the primary unit for virtual cluster 2.

```
get system ha status
Model: 5000
Mode: a-p
Group: 0
Debug: 0
ses_pickup: disable
Master:128 5001_slot_7 FG50012205400050 0
Slave :200 5001_slot_11 FG50012204400045 1
number of vcluster: 2
vcluster 1: work 10.0.0.2
Master:1 FG50012205400050
Slave :0 FG50012204400045
vcluster 2: standby 10.0.0.1
Master:0 FG50012205400050
Slave :1 FG50012204400045
```

This example shows three sets of indexes. The indexes in lines six and seven are still used by the `execute ha manage` command. The indexes on lines ten and eleven are for the primary and subordinate units in virtual cluster 1 and the indexes on the last two lines are for virtual cluster 2.

History

FortiOS v3.0 MR2 New command.

Related topics

- system ha
- execute ha disconnect
- execute ha manage
- execute ha synchronize

system info admin ssh

Use this command to display information about the SSH configuration on the FortiGate unit such as:

- the SSH port number
- the interfaces with SSH enabled
- the hostkey DSA fingerprint
- the hostkey RSA fingerprint

Syntax

```
get system info admin ssh
```

Example

This shows sample output.

```
# get system info admin ssh
SSH v2 is enabled on port 22
SSH is enabled on the following 1 interfaces:
        internal
SSH hostkey DSA fingerprint = cd:e1:87:70:bb:f0:9c:7d:e3:7b:73:f7:44:23:a5:99
SSH hostkey RSA fingerprint = c9:5b:49:1d:7c:ba:be:f3:9d:39:33:4d:48:9d:b8:49
```

History

FortiOS v3.0 MR2	New.
FortiOS v3.0 MR4	Output changed - added SSH hostkey RSA fingerprint.

Related topics

- system accprofile
- execute disconnect-admin-session

system info admin status

Use this command to display administrators that are logged into the FortiGate unit.

Syntax

```
get system info admin status
```

Example

This shows sample output.

```
Index  User name   Login type  From
  0    admin       CLI         ssh(172.20.120.16)
  1    admin       WEB         172.20.120.16
```

`Index`	The order the administrators logged in.
`User name`	The name of the user account logged in.
`Login type`	Which interface was used to log in.
`From`	The IP address this user logged in from.

History

FortiOS v3.0 MR2 New.

Related topics

- get system info admin ssh

system interface physical

Use this command to list information about the unit's physical network interfaces.

Syntax

```
get system interface physical
```

The output looks like this:

```
# get system interface physical
== [onboard]
        ==[dmz1]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                status: down
                speed: n/a
        ==[dmz2]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                status: down
                speed: n/a
        ==[internal]
                mode: static
                ip: 172.20.120.146 255.255.255.0
                status: up
               speed: 100
        ==[wan1]
                mode: pppoe
                ip: 0.0.0.0 0.0.0.0
                status: down
                speed: n/a
        ==[wan2]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                status: down
                speed: n/a
        ==[modem]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                status: down
                speed: n/a
```

History

FortiOS v4.0 New.

system performance status

Use this command to display FortiGate CPU usage, memory usage, network usage, sessions, virus, IPS attacks, and system up time.

Syntax

```
get system performance status
```

Example

The output looks like this:

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle
Memory states: 18% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 1 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 6 sessions in 10 minutes, 5 sessions
in 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 9days, 22 hours, 0 minutes
```

`CPU states`	The percentages of CPU cycles used by user, system, nice and idle categories of processes. These categories are: • `user` -CPU usage of normal user-space processes • `system` -CPU usage of kernel • `nice` - CPU usage of user-space processes having other-than-normal running priority • `idle` - Idle CPU cycles Adding user, system, and nice produces the total CPU usage as seen on the CPU widget on the web-based system status dashboard.
`Memory states`	The percentage of memory used.
`Average network usage`	The average amount of network traffic in kbps in the last 1, 10 and 30 minutes.
`Average sessions`	The average number of sessions connected to the FortiGate unit over the list 1, 10 and 30 minutes.
`Virus caught`	The number of viruses the FortiGate unit has caught in the last 1 minute.
`IPS attacks blocked`	The number of IPS attacks that have been blocked in the last 1 minute.
`Uptime`	How long since the FortiGate unit has been restarted.

History

FortiOS v3.0	Added.
FortiOS v3.0 MR2	Changed to ‘get system performance status’ and moved from ‘system’ to ‘get’ chapter.
FortiOS v3.0 MR3	Output of command changed to include more CPU information, average network traffic, average sessions, viruses caught, and IPS attacks blocked.

system session list

Command returns a list of all the sessions active on the FortiGate unit. or the current virtual domain if virtual domain mode is enabled.

Syntax

```
get system session list
```

Example

The output looks like this:

```
PROTO     EXPIRE  SOURCE          SOURCE-NAT   DESTINATION    DESTINATION-NAT
tcp     0       127.0.0.1:1083    -            127.0.0.1:514    -
tcp     0       127.0.0.1:1085    -            127.0.0.1:514    -
tcp     10      127.0.0.1:1087    -            127.0.0.1:514    -
tcp     20      127.0.0.1:1089    -            127.0.0.1:514    -
tcp     30      127.0.0.1:1091    -            127.0.0.1:514    -
tcp     40      127.0.0.1:1093    -            127.0.0.1:514    -
tcp     60      127.0.0.1:1097    -            127.0.0.1:514    -
tcp     70      127.0.0.1:1099    -            127.0.0.1:514    -
tcp     80      127.0.0.1:1101    -            127.0.0.1:514    -
tcp     90      127.0.0.1:1103    -            127.0.0.1:514    -
tcp     100     127.0.0.1:1105    -            127.0.0.1:514    -
tcp     110     127.0.0.1:1107    -            127.0.0.1:514    -
tcp     103     172.20.120.16:3548 -           172.20.120.133:22 -
tcp     3600    172.20.120.16:3550 -           172.20.120.133:22 -
udp     175     127.0.0.1:1026    -            127.0.0.1:53     -
tcp     5       127.0.0.1:1084    -            127.0.0.1:514    -
tcp     5       127.0.0.1:1086    -            127.0.0.1:514    -
tcp     15      127.0.0.1:1088    -            127.0.0.1:514    -
tcp     25      127.0.0.1:1090    -            127.0.0.1:514    -
tcp     45      127.0.0.1:1094    -            127.0.0.1:514    -
tcp     59      127.0.0.1:1098    -            127.0.0.1:514    -
tcp     69      127.0.0.1:1100    -            127.0.0.1:514    -
tcp     79      127.0.0.1:1102    -            127.0.0.1:514    -
tcp     99      127.0.0.1:1106    -            127.0.0.1:514    -
tcp     109     127.0.0.1:1108    -            127.0.0.1:514    -
tcp     119     127.0.0.1:1110    -            127.0.0.1:514    -
```

PROTO	The transfer protocol of the session.
EXPIRE	How long before this session will terminate.
SOURCE	The source IP address and port number.
SOURCE-NAT	The source of the NAT. '-' indicates there is no NAT.
DESTINATION	The destination IP address and port number.
DESTINATION-NAT	The destination of the NAT. '-' indicates there is no NAT.

History

FortiOS v3.0 MR2 New command.

FortiOS v3.0 MR6 Now per VDOM.

system session status

Command returns the number of active sessions on the FortiGate unit, or if virtual domain mode is enabled it returns the number of active sessions on the current VDOM. In both situations it will say ‘the current VDOM’.

Syntax

```
get system session status
```

Example

The output looks like this:

```
The total number of sessions for the current VDOM: 31
```

History

FortiOS v3.0 MR6 New command.

system status

Use this command to display system status information including:

- FortiGate firmware version, build number and branch point
- virus and attack definitions version
- FortiGate unit serial number and BIOS version
- log hard disk availability
- host name
- operation mode
- virtual domains status: current VDOM, max number of VDOMs, number of NAT and TP mode VDOMs and VDOM status
- current HA status
- system time

Syntax

```
get system status
```

Example output

```
Version: Fortigate-800 v4.0.1,build0056,081107
Virus-DB: 8.00631(2008-01-15 14:27)
IPS-DB: 2.00542(2008-09-04 23:08)
Serial-Number: FGT8002805030003
BIOS version: 03000300
Log hard disk: Available
Hostname: FGT8002805030003
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 4 in NAT mode, 0 in TP mode
Virtual domain configuration: enable
FIPS-CC mode: disable
Current HA mode: standalone
Distribution: International
Branch point: 056
Release Version Information: Beta 1
System time: Mon Nov 24 16:25:56 2008
```

History

FortiOS v3.0	Added.
FortiOS v3.0 MR2	Moved from ‘system’ to ‘get’ chapter.

Related topics

- hardware status

system wireless detected-ap

Use this command to view the list of access points detected in SCAN mode or when `bg-scan` is set to `enable`. For more information see “system wireless settings” on page 540.

Syntax

```
get system wireless detected-ap
```

Example output

```
SSID            BSSID             CHAN RATE  S:N    INT CAPS ACT LIVE AGE
Distil_G        00:1b:2f:9f:6a:0b   1   54M 19:0    100 EPSs  Y  10  0 WPA
VLAN2Z          00:1d:70:59:a6:40   6   54M  6:0    100 EPSs  Y  10  0 RSN
0...            00:16:46:9b:ba:d0  11   54M  3:0    100 ES    Y  10  0 WME
HCS-users       00:17:c5:00:f0:31   7   54M  2:0    100 EPs   Y  10  10 WPA
training        00:12:bf:14:fa:82   2   54M 43:0    100 EPSs  Y  7   7 WPA WME
0...            00:16:46:9b:ba:b0   9   54M 17:0    100 ESs   Y  6   6 WME
dixon           00:11:50:d5:d6:c2  11   54M  7:0    100 EPs   Y  0   0
```

History

FortiOS v4.0.0 New.

Related topics

- system wireless ap-status
- system wireless settings

user adgrp

Use this command to list Directory Service user groups.

Syntax

```
get user adgrp [<dsgroupname>]
```

If you do not specify a group name, the command returns information for all Directory Service groups. For example:

```
== [ DOCTEST/Cert Publishers ]
name: DOCTEST/Cert Publishers    server-name: DSserv1
== [ DOCTEST/Developers ]
name: DOCTEST/Developers    server-name: DSserv1
== [ DOCTEST/Domain Admins ]
name: DOCTEST/Domain Admins    server-name: DSserv1
== [ DOCTEST/Domain Computers ]
name: DOCTEST/Domain Computers    server-name: DSserv1
== [ DOCTEST/Domain Controllers ]
name: DOCTEST/Domain Controllers    server-name: DSserv1
== [ DOCTEST/Domain Guests ]
name: DOCTEST/Domain Guests    server-name: DSserv1
== [ DOCTEST/Domain Users ]
name: DOCTEST/Domain Users    server-name: DSserv1
== [ DOCTEST/Enterprise Admins ]
name: DOCTEST/Enterprise Admins    server-name: DSserv1
== [ DOCTEST/Group Policy Creator Owners ]
name: DOCTEST/Group Policy Creator Owners    server-name: DSserv1
== [ DOCTEST/Schema Admins ]
name: DOCTEST/Schema Admins    server-name: DSserv1
```

If you specify a Directory Service group name, the command returns information for only that group. For example:

```
name                : DOCTEST/Developers
server-name         : ADserv1
```

The `server-name` is the name you assigned to the Directory Service server when you configured it in the `user fsae` command.

History

FortiOS v3.0 New.

Related topics

- user fsae
- execute fsae refresh

vpn ssl monitor

Use this command to display information about logged in SSL VPN users and current SSL VPN sessions.

Syntax

```
get vpn ssl monitor
```

Output

```
FortiGate 300 # get vpn ssl monitor

SSL-VPN Login Users:
Index    User    Auth Type      Timeout From    HTTP in/out    HTTPS in/out

SSL-VPN sessions:
Index    User    Source IP      Tunnel/Dest IP
```

History

FortiOS v3.0 New.

Related topics

- vpn ssl settings

wireless-controller scan

Use this command to view the list of access points detected when `ap-scan` is set to `bgscan` or `fgscan`. For more information see wireless-controller wtp.

Syntax

```
get wireless-controller scan
```

Example output

```
SSID            BSSID             CHAN RATE  S:N    INT CAPS ACT LIVE AGE
Distil_G        00:1b:2f:9f:6a:0b   1   54M 19:0    100 EPSs  Y  10  0 WPA
VLAN2Z          00:1d:70:59:a6:40   6   54M  6:0    100 EPSs  Y  10  0 RSN
0...            00:16:46:9b:ba:d0  11   54M  3:0    100 ES    Y  10  0 WME
HCS-users       00:17:c5:00:f0:31   7   54M  2:0    100 EPs   Y  10  10 WPA
training        00:12:bf:14:fa:82   2   54M 43:0    100 EPSs  Y  7   7 WPA WME
0...            00:16:46:9b:ba:b0   9   54M 17:0    100 ESs   Y  6   6 WME
dixon           00:11:50:d5:d6:c2  11   54M  7:0    100 EPs   Y  0   0
```

History

FortiOS v4.0 MR1 New.

Related topics

- wireless-controller wtp

wireless-controller status

Use this command to list the physical AP (WTP) firmware images stored on the wireless-controller.

Syntax

```
get wireless-controller status
```

History

FortiOS v4.0 MR1 New.

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

www.fortinet.com

www.fortinet.com