FortiOS™ CLI Reference

FortiOS 4.0 MR2

Visit http://support.fortinet.com to register your FortiOS product. By registering you can receive product updates, technical support, and FortiGuard services.

FortiOS CLI Reference

FortiOS 4.0 MR2

30 June 2010

01-420-99686-20100630

Trademarks

Contents

Introduction

This document describes FortiOS 4.0 MR2 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI).

- How this guide is organized
- Document conventions
- Registering your Fortinet product
- Fortinet products End User License Agreement
- Customer service and technical support
- Training
- Documentation

How this guide is organized

Most of the chapters in this document describe the commands for each configuration branch of the FortiOS CLI. The command branches and commands are in alphabetical order.

This document also contains the following sections:

What’s new describes changes to the 4.0 MR2 CLI.

execute describes execute commands.

get describes get commands.

Availability of commands and options

Some FortiOS CLI commands and options are not available on all FortiGate units. The CLI displays an error message if you attempt to enter a command or option that is not available. You can use the question mark ‘?’ to verify the commands and options that are available.

Commands and options may not be available for the following reasons:

- **FortiGate model**. All commands are not available on all FortiGate models. For example, low end FortiGate models do not support the `aggregate` option of the `config system interface` command.
- **Hardware configuration**. For example, some AMC module commands are only available when an AMC module is installed.
- **FortiOS Carrier, FortiGate Voice**, **FortiWiFi etc**. Commands for extended functionality are not available on all FortiGate models. The CLI Reference includes commands only available for FortiWiFi units, FortiOS Carrier, and FortiGate Voice units

Document 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.

Cautions, Notes and Tips

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

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

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

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

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*. **Note:** Links typically go to the most recent version. To access earlier releases, go to http://docs.fortinet.com/. This link appears at the bottom of each page of this document.

CLI command syntax

See "Command syntax" on page 33.

Registering your Fortinet product

Before you begin configuring and customizing features, 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.

Fortinet products End User License Agreement

See the *Fortinet products End User License Agreement*.

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?

Training

Fortinet Training Services provides courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email training@fortinet.com.

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 Base

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

What’s new

As the FortiOS Handbook is being developed, the *FortiGate CLI Reference* is becoming a dictionary of FortiOS CLI commands. Examples have been removed from this CLI Reference and command explanations are being more sharply focused on defining the command and its options, ranges, defaults and dependencies. The CLI Reference now includes FortiOS Carrier commands and future versions will include FortiGate Voice commands. Also command histories have been removed.

These changes are in progress and will be completed in future versions of this document.

The table below lists CLI commands and options that have been added to FortiOS 4.0 MR2. This version of the CLI Reference does not include all FortiOS 4.0 MR2 CLI changes. A more complete version of this document is scheduled to be published in early May 2010.

Command	Change
`config antivirus profile`	New command for configuring antivirus profiles for firewall policies.
`config antivirus settings`	
`set default-db flow-based`	New option. Enables flow-based antivirus scanning.
`set default-db extreme`	New option. Enables the extreme virus database.
`set quarantine-quota`	New option. Set the amount of disk space available for quarantining files.
`config application list`	New options: chart {enable | disable}, unknown-application-action {block | pass}, and unknown-application-log {disble | enable}. shaper <shaper_str> and shaper-reverse <shaper_str> now available for all applications.
`set block-long-chat`	This option has been removed.
`set imoversizechat`	This option has been removed.
`config dlp compound`	
`clone <name1> <name2>`	New command. Clone an existing DLP compound rule. Cloning can be used for upgrading default DLP regular expressions to new improved ones.
`config dlp rule`	
`clone <name1> <name2>`	New command. Clone an existing DLP. Cloning can be used for upgrading default DLP regular expressions to new improved ones.
`config dlp sensor`	
`clone <name1> <name2>`	New command. Clone an existing DLP sensor. Cloning can be used for upgrading default DLP regular expressions to new improved ones.
`config endpoint-control app-detect rule-list`	
`set status`	New status options `not-installed and not-running`.
`config endpoint-control profile`	
`set capability-based-check`	New option. Enable to allow non-compliant endpoint access.
`config firewall central NAT`	New command. Used for creating NAT rules and NAT mapping that are setup by the global firewall table
`status`	Enable or disable NAT rule.
`orig-addr`	Define source ip address

Command	**Change**
nat-ippool	Define NAT ip address/ip pool
orig-port	Define source port number
nat-port	Define translated port number or range of ports.
config firewall profile	This command has been removed and its functionality moved to the config antivirus profile, config firewall policy and other UTM-related commands.
config firewall profile-group	New command to configure UTM profile groups added.
application-charts	New field for setting application chart types. There are three pre-defined chart types available; top10-app, top10-media-user and top10-p2p-user.
config firewall profile-protocol-options	New command to configure UTM protocol option profiles added. When unset options <option_name> is used, <option_name> can be left blank for all protocols (http, https, smtp, pop3, imap. ftp, nntp, pop3s, smtps, imaps and im)
config firewall policy, policy6	Added options to select UTM profiles in firewall policies and in identity-based policies. For example utm-status {disable | enable}, profile-type {group | single}, profile-group {group | single}, profile-protocol-options <name_str>, av-profile <name_str>, webfilter-profile <name_str>, etc.
config service custom	Port 0 is added for udp-portrange, tcp-portrange and sctp-portrange and the new port range is 0-65535.
config firewall shaper per-ip-shaper	Command changed.
config firewall shaper traffic-shaper	Command changed.
config firewall ssl setting	
no-matching-cipher-action	Bypass or drop SSL traffic when unsupported cipher is being used by the server.
config firewall vip	
set ssl-client-recognition	New option for allowing an SSL client to renegotiate or aborting any SSL connection that attempts to renegotiate. This option appears only if type is server-load-balance and server-type is ssl.
config ips DoS	
set quarantine-log	New option. Enables NAC quarantine logging.
config ips sensor	
set log-packet	New option. Enables packet logging for ips filters.
config log disk filter	
set event	Removed. Use new config log eventfilter command.
config log eventfilter	New command. Configures event logging.
config log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting	
set source-ip	New field, Removed. Enter the source IP address for the FortiAnalyzer, FortiAnalyzer2 and FortiAnalyzer3 units.
set gui-display	New field, Enable or disable to display FortiAnalyzer Reports on the web-based manager.
config log disk setting	
set source-ip	Enter the source IP address of the disk log uploading.
set storage	Enter a name for the storage log file. This option is only available when the current vdom is the management vdom.

Command	Change
`set log-quota`	New field. Enter then amount (in MB) of disk space allocated for disk logging.
`set dlp-archive-quota`	New field. Enter then amount (in MB) of disk space allocated for DLP logs.
`set report-quota`	New field. Enter then amount (in MB) of disk space allocated for report logs.
`set ips-packet-quota`	New field. Enter then amount (in MB) of disk space allocated for IPS packet archives.
`config log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter`	
`set web-filter-ftgd-quota`	New field. Enable or disable logging FortiGuard quota levels.
`set web-filter-ftgd-quota-counting`	New field. Enable or disable logging FortiGuard quota counting messages.
`set web-filter-ftgd-quota-expired`	New field. Enable or disable logging FortiGuard quota expired messages.
`config log memory filter`	
`set event`	Removed. Use new `config log eventfilter` command.
`config log {syslogd | syslogd2 | syslogd3} setting`	
`set ip-source`	New field. Enter the corresponding source IP address for syslogd, syslog2 and syslog3,
`config netscan`	New command branch. Configure the network vulnerability scanner.
`config router isis`	New command. Configure ISIS routing.
`config spamfilter profile`	New command for configuring email filtering profiles for firewall policies.
`config system admin`	
`config dashboard`	
`edit storage`	New option, Hard disk storage widget type is added to the dashboard.
`config system amc-slot`	New command to configure settings for the modules installed in AMC slots.
`config system alertemail`	
`set source-ip`	New field. Enter the SMTP server source IP address.
`config system central-management`	
`set source-ip`	New field. Enter the source IP address to use when connecting to FortiManager.
`config system dhcp server`	DHCP servers have index numbers and include the new `dns-server` option. You can add multiple IP address ranges to a DHCP server using the `config ip-range` subcommand.
`config system gre-tunnel`	New command to configure the tunnel for a GRE interface.
`set system interface <interface_name>`	Can now select an IPSec VPN interface.
`config system interface`	
`set external`	This option is now available in FortiOS, used to be limited to FortiCarrier.
`set npu-fastpath`	New field. Allows disabling or enabling NP2 fast path acceleration.

Command	Change
set poe	New field. Allows disabling or enabling PoE (Power over Ethernet). This option is only available on FortiGate units featuring PoE.
config system global	
set endpoint-control-fds-access	New field. Enable or disable access to FortiGuard servers for non-compliant endpoints.
set ipsec-hmac-offload	Enable to offload IPsec HMAC processing to hardware or disable to not offload IPsec HMAC processing to hardware.
set scanunit-count	Change the number of scanunits. For advanced users.
set revision-backup-on-logout	Back up the latest configuration revision when the administrator logs out.
config system sflow	New command. Configures sFlow settings.
config system snmp community	New field: source-ip. Enter the source IP address for SNMP traps sent by the FortiGate unit.
config system storage	New command. Configures disk storage settings.
config system interface	
set polling-interval	New Field. Set the sFlow polling interval.
set sample-direction	New Field. Set the sFlow sampling direction.
set sample-rate	New field. Set the sFlow sample rate.
set sflow-sample	New field to add sFlow sampling to an interface.
config system settings	
set wccp-cache-engine	New field. Configure the FortiGate unit to operate as a WCCP cache engine.
config system resource-limits	
set webproxy set log-disk-quota	New fields. Set a limit to the number of explicit web proxy users and the amount of log disk space that can be used globally.
config system vdom-property	
set webproxy set log-disk-quota	New fields. Set a limit to the number of explicit web proxy users and the amount of log disk space that can be used for a VDOM.
config system wccp	New options to support WCCP cache engine mode.
config system vdom-sflow	New command. Configures sFlow settings for non-management VDOMs.
config user group edit <groupname>	
set ldap-memberof	Removed. Use the config match subcommand.
config match	New subcommand. Configure a matching user group on a authentication server.
set group-name	New field. Set the matching group name on the authentication server.
set server-name	New field. Set the authentication server name.
config user ldap edit <server_name>	
set group	Removed. Use the config user group subcommand config match.
set password-expiry-warning	New field. Use this option to enable or disable password expiry warnings.
set password-renewal	New field. Use this option to enable or disable online password renewal.

Command	Change
`config user radius`	
`  edit <server_name>`	
`    set use-group-for-profile`	Removed. Use the `config user group` subcommand `config match`.
`config voip profile`	New command. Configures SIP and SCCP VoIP profiles for firewall policies.
`config vpn ssl web portal`	
`  config widget`	
`    set exclusive-routing`	New field. Enabling exclusive-routing adds options to allow client traffic flow control.
`config wanopt webcache`	
`    set cache-exemption`	New option. Enable or disable cache exemption list.
`      config cache-exemption-list`	New subcommand. Configure a list of URLs for exemption.
`          set url-pattern`	New field. Set a URL or IP address.
`config webfilter fortiguard`	
`  set ovrd-auth-hostname`	New field. Enter a host name to use for FortiGuard Web Filter HTTPS override authentication.
`  set ovrd-auth-cert`	New field. Enter a certificate name to use for FortiGuard Web Filter HTTPS override authentication.
`config webfilter profile`	New command for configuring web filtering profiles for firewall policies.
`config webfilter urlfilter`	New `pass` action that is similar to the `exempt` action.
`config web-proxy explicit`	New options added.
`execute backup`	Display information about a security processing module installed in a AMC slot.
`execute backup log`	New `backup log` feature. Back up the specified type of log file from either hard disk or memory to FTP or TFTP server.
`execute log recreate-sqldb`	New command for recreating SQL log database
`execute restore vcn`	New command for restoring VCM engine from an FTP or TFTP server.

```
New execute commands
```

```
execute disk
execute netscan
execute npu-cli
execute tac report
```

Command	Change
New get commands	
get firewall dnstranslation	
get firewall iprope appctrl	
get firewall iprope list	
get firewall proute	
grep	
get hardware cpu	
get hardware memory	
get hardware nic	
get hardware npu	
get hardware status	
get ips session	
get ipsec tunnel list	
get netscan settings	
get router info kernel	
get router info vrrp	
get system auto-update	
get system performance firewall	
get system performance top	
get system startup-error-log	
get system session-helper-info list	
get test	
get vpn status concentrators	
get vpn status ike	
get vpn status ipsec	
get vpn status l2tp	
get vpn status pptp	
get vpn status ssl	
get vpn status tunnel	
get webfilter ftgd-statistics	

alertemail

Use the `config alertemail` command 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.

This chapter describes the following command:

setting

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 327 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.

Variable	Description	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`

antivirus

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

This chapter describes the following commands:

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.

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 | intercept}
        set active {ftp http im imap imaps mm1 mm3 mm4 mm7 nntp pop3 pop3s
            smtp smtps}
        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 the file pattern header list.	
`<filepattern_string>`	The name of the file pattern being configured. This can be any character string.	
`action {allow | block | intercept}`	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. • Select `intercept` to configure FortiOS Carrier to allow matching files, with a copy sent to a quarantine. Note that the `store-intercepted` command in `config antivirus quarantine` must also be configured to quarantine intercepted files. Enable `intercept-log` in a protocol options profile to write a log message when files are intercepted.	`block`
`active {ftp http im imap imaps mm1 mm3 mm4 mm7 nntp pop3 pop3s smtp smtps}`	The `action` specified will affect the file pattern in the selected protocols. MM1, MM3, MM4, and MM7 traffic types are supported by FortiOS Carrier.	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`

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`

mms-checksum

Use this command in FortiOS Carrier to create a list of attachment checksum values. Messages containing these attachments can be blocked by the MMS profile.

Syntax

```
config antivirus mms-checksum
  edit <entry_id>
    set comment <comment_str>
    config entries
      edit <entry_name>
        set checksum <checksum_value>
        set status {enable | disable}
      end
    end
```

Variable	Description	Default
`comment <comment_str>`	Optionally, enter a comment.	
`<entry_name>`	Enter a name for the blockable item.	
`checksum <checksum_value>`	Enter the checksum value.	
`status {enable | disable}`	Enable the entry.	`enable`

notification

Use this command for FortiOS Carrier to configure the viruses that trigger notification messages.

A notification list must be added to the MMS profile to generate notification messages.

Syntax

```
config antivirus notification
  edit <list_id_int>
    set name <name_str>
    set comment <comment_str>
    config entries
      edit <virus_str>
        set prefix {enable | disable}
        set status {enable | disable}
    end
end
```

Keywords and variables	Description	Default
`<list_id_int>`	Enter the ID number of the list to edit. Each notification list has a unique ID number. Enter `edit ?` to view all the lists with their ID numbers.	No default.
`name <name_str>`	Enter a name for the notification list. If the list is new, you must enter a name. You can also use this command to change the name of an existing notification list.	No default.
`comment <comment_str>`	Enter an optional comment for the notification list. You can also use this command to change the name of an existing notification list.	No default.
`<virus_str>`	Enter the virus pattern to edit an existing list entry, or enter a new virus pattern to create a new list entry.	No default.
`prefix {enable | disable}`	Enable to match the virus pattern with the beginning of any virus name. Disable to match the virus pattern with all of any virus name. For example, a pattern of `BDoor.ACJ!tr.bdr` with the prefix setting disabled will have the FortiGate unit check for a virus with that exact name. With the prefix setting enabled, a prefix match entry for `BDoor` will generate a notification message for any of the dozens of virus variants starting with `BDoor`.	`enable`
`status {enable | disable}`	If required, you can disable a notification entry without removing it from the list. The FortiGate unit will ignore the list entry. By default, all list entries are enabled as soon as you create them.	`enable`

profile

Use this command to configure UTM antivirus profiles for firewall policies. Antivirus profiles configure how virus scanning is applied to sessions accepted by a firewall policy that includes the antivirus profile.

Syntax

```
config antivirus profile
  edit <name_str>
    set comment <comment_str>
    set filepattable <filepattern_list_int>
    set av-virus-log {disable | enable}
    set av-block-log {disable | enable}
      config config {http | https | ftp | imap | imaps | pop3 | pop3s | smtp
          | smtps | nntp | im}
        set options {avmonitor | avquery | file-filter | quarantine | scan |
            strict-file}
        set avdb {default | extended | normal | flow-based}
      config config nac-quar
        set infected {none | quar-interface | quar-scr-ip}
        set log {disable | enable}
    end
end
```

Variable	Description	Default
`<name_str>`	Enter the name of the antivirus profile.	
`comment <comment_str>`	Optionally enter a description of up to 63 characters of the antivirus profile.	
`filepattable <filepattern_list_int>`	A unique number to identify the antivirus file pattern list added to the antivirus profile.	`0`
`av-virus-log {disable | enable}`	Enable or disable logging for virus scanning.	`disable`
`av-block-log {disable | enable}`	Enable or disable logging for antivirus file pattern blocking.	`disable`

config {http | https | ftp | imap | imaps | pop3 | pop3s | smtp | smtps | nntp | im}

Configure virus scanning options for the selected protocol.

Variable	Description	Default
`options {avmonitor	avquery	file-filter	quarantine	scan	strict-file}`	Select one or more options apply to virus scanning for the protocol. To select more than one, enter the option names separated by a space. Some options are only available for some protocols. `avmonitor` log detected viruses, but allow them through the firewall without modification. Available for FortiOS Carrier. `avquery` use the FortiGuard AV query service. `file-filter` apply the antivirus file pattern list to the protocol. `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 transferred using this protocol for viruses. `strict-file` perform strict checking for viruses by blocking files that include query strings. This more thorough checking can effectively block some web sites with elaborate scripting using `.exe` or `.dll` files if those patterns are blocked. Available for the HTTP and HTTPS protocols.	
`avdb {default	extended	normal	flow-based}`	Select the antivirus database to use for the protocol. `default` use the database selected in "antivirus settings" on page 45. `extended` select the extended virus database, which includes both In the Wild viruses and a large collection of zoo viruses that are no longer seen in recent virus studies. It is suitable for an enhanced security environment. `extreme` select the extreme virus database, which includes both In the Wild viruses and all available zoo viruses that are no longer seen in recent virus studies. It is suitable for an enhanced security environment. `flow-based` select the flow-based virus database, which includes In the Wild viruses and some commonly seen viruses on the network. Flow-based virus scan is an alternate to the file-based virus scan. It provides better performance but lower coverage rate compared to file-based virus scan. `normal` select the regular virus database, which includes In the Wild viruses and most commonly seen viruses on the network. For regular virus protection, it is sufficient to use this database.	`default`

config nac-quar

Configure NAC quarantine virus scanning options.

Variable	Description	Default
`infected {none	quar-interface	quar-scr-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`
`log {disable	enable}`	Enable or disabling logging for NAC quarantine.	`disable`

quarantine

Use this command to set file quarantine options. FortiGate units with a hard disk or a connection to a FortiAnalyzer unit can quarantine files. FortiGate features such as virus scanning can quarantine files.

Syntax

```
config antivirus quarantine
  set agelimit <hours_int>
  set destination {disk | FortiAnalyzer | NULL}
  set drop-blocked {ftp http imap mm1 mm3 mm4 mm7 nntp pop3 smtp}
  set drop-heuristic {ftp http im imap mm1 mm3 mm4 mm7 nntp pop3 smtp}
  set drop-infected {ftp http im imap mm1 mm3 mm4 mm7 nntp pop3 smtp}
  set drop-intercepted {ftp http imap mm1 mm3 mm4 mm7 pop3 smtp}
  set enable-auto-submit {disable | enable}
  set lowspace {drop-new | ovrw-old}
  set maxfilesize <MB_int>
  set quarantine-quota <MB_int>
  set sel-status {fileblocked heuristic}
  set store-blocked {ftp http imap mm1 mm3 mm4 mm7 nntp pop3 smtp}
  set store-heuristic {ftp http im imap mm1 mm3 mm4 mm7 nntp pop3 smtp}
  set store-infected {ftp http im imap mm1 mm3 mm4 mm7 nntp pop3 smtp}
  set store-intercepted {ftp http imap mm1 mm3 mm4 mm7 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. This option appears when destination is not set to `NULL`.	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 mm1 mm3 mm4 mm7 nntp pop3 smtp}`	Do not quarantine blocked files found in traffic for the specified protocols. The files are deleted. MM1, MM3, MM4, and MM7 traffic types supported only in FortiOS Carrier.	`imap` `nntp`

`drop-heuristic {ftp http im imap mm1 mm3 mm4 mm7 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.
	MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier.
		`http`
		`im`
		`imap`
		`nntp`
		`pop3`
		`smtp`

`drop-infected {ftp http im imap mm1 mm3 mm4 mm7 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.
	MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier.
		`im`
		`imap`
		`nntp`

Variable	Description	Default
`drop-intercepted {ftp http imap mm1 mm3 mm4 mm7 pop3 smtp}`	For FortiOS Carrier, do not quarantine intercepted files found in traffic for the specified protocols. The files are deleted.	imap smtp pop3 http ftp mm1 mm3 mm4 mm7
`enable-auto-submit {disable | enable}`	Enable or disable automatic submission of the quarantined files matching the `use-fpat` or `use-status` settings. This option appears when destination is not set to `NULL`.	`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. This option appears when `destination` is not set to `NULL`.	`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
`quarantine-quota <MB_int>`	Set the antivirus quarantine quota in MB, which is the amount of disk space to reserve for quarantining files.	0
`sel-status {fileblocked heuristic}`	Configure the status used for automatic uploading of quarantined files. This option appears when `destination` is not set to `NULL`.	No default.
`store-blocked {ftp http imap mm1 mm3 mm4 mm7 nntp pop3 smtp}`	Quarantine blocked files found in traffic for the specified protocols. NNTP support for this field will be added in the future. HTTP, FTP, MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier.	No default.
`store-heuristic {ftp http im imap mm1 mm3 mm4 mm7 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. MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier.	No default.
`store-infected {ftp http im imap mm1 mm3 mm4 mm7 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. MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier.	No default.
`store-intercepted {ftp http imap mm1 mm3 mm4 mm7 pop3 smtp}`	Quarantine intercepted FortiOS Carrier files found in traffic of the specified protocols.	imap smtp pop3 http ftp mm1 mm3 mm4 mm7
`use-fpat {enable | disable}`	Enable or disable using file patterns to select quarantined files for automatic uploading. See "antivirus quarfilepattern" on page 43 for information on how to configure the file patterns used for automatic uploading. This option appears when `destination` is not set to `NULL`.	`disable`
`use-status {enable | disable}`	Enable or disable using file status to select quarantined files for automatic uploading. This option appears when `destination` is not set to `NULL`.	`disable`

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.

Syntax

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

Variable	Description	Default
`<pattern_str>`	The file pattern to be quarantined. The pattern can include the asterisk `*` wildcard character. For example, `*.bat` matches all files with the `bat` file extension.	
`status {disable | enable}`	Enable or disable using a file pattern.	`disable`

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.

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`

settings

Use this command to select the default antivirus database and to enable or disable grayware detection as part of antivirus scanning.

Syntax

```
config antivirus settings
  set default-db {extended | extreme | flow-based | normal}
  set grayware {enable | disable}
  end
```

Variable	Description	Default
`default-db {extended	extreme	flow-based	normal}`	Select the default antivirus database to use for virus scanning. You can override the default database for specific protocols in the antivirus profile, see "antivirus profile" on page 39. `extended` select the extended virus database, which includes both In the Wild viruses and a large collection of zoo viruses that are no longer seen in recent virus studies. It is suitable for an enhanced security environment. `extreme` select the extreme virus database, which includes both In the Wild viruses and all available zoo viruses that are no longer seen in recent virus studies. It is suitable for an enhanced security environment. `flow-based` select the flow-based virus database, which includes In the Wild viruses and some commonly seen viruses on the network. Flow-based virus scan is an alternate to the file-based virus scan. It provides better performance but lower coverage rate compared to file-based virus scan. `normal` select the regular virus database, which includes In the Wild viruses and most commonly seen viruses on the network. For regular virus protection, it is sufficient to use this database.	`normal`
`grayware {enable	disable}`	Enable or disable grayware detection. Grayware includes adware, dial, downloader, hacker tool, keylogger, RAT and spyware.	`disable`

application

Use these commands to configure application control.

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-audio {enable | disable}
        set block-encrypt {enable | disable}
        set block-file {enable | disable}
        set block-im {enable | disable}
        set block-photo {enable | disable}
        set category {<cat_int> | All}
        set comment <comment_string>
        set im-no-content-summary {enable | disable}
        set inspect-anyport {enable | disable}
        set log {disable | enable}
        set log-packet {disable | enable}
        set other-application-action {block | pass}
        set other-application-log {enable | disable}
        set session-ttl <ttl_int>
        set shaper <shaper_str>
        set shaper-reverse <shaper_str>
      end
    end
    set chart {enable | disable}
    set comment <comment_string>
    set log {disable | enable}
    set other-application-action {block | pass}
    set other-application-log {enable | disable}
    set unknown-application-action {block | pass}
    set unknown-application-log {disble | enable}
  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`

Variable	Description	Default
`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-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-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`
`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`
`chart {enable | disable}`	Enable or disable monitoring for the applications in the application control list.	`disable`
`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`
`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`
`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 for an application control list to have the FortiGate unit log the occurrence and the action taken if traffic from any of the applications in the application control list is detected.	`enable`
`log-packet {disable | enable}`	Enable or disable packet logging for an application in the application control list.	`disable`
`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`
`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`
`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 <shaper_str>`	Enter the name of a traffic shaper to enable traffic shaping for this application.	No default
`shaper-reverse <shaper_str>`	Enter the name of a traffic shaper to enable reverse traffic shaping for this application.	No default

Variable	Description	Default
`unknown-application-action {block | pass}`	Pass or block applications that have not been added to this application list.	pass
`unknown-application-log {disble | enable}`	Enable or disable recording log messages when an application not added to the application list is detected.	`disable`

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

dlp

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
  clone clone <name1> <name2>
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 56.	No default.
`protocol {email | ftp | http | im | nntp}`	Select the protocol to which this compound rule applies.	No default.

Variable	Description	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.
`clone <name1> <name2>`	Clone an existing DLP compound rule. Cloning can be used for upgrading default DLP regular expressions to new improved ones.	

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
  clone clone <name1> <name2>
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`
`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`

Variable	Description	Default
`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`
`clone <name1> <name2>`	Clone an existing DLP rule. Cloning can be used for upgrading default DLP regular expressions to new improved ones.	

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.

Syntax

```
config dlp sensor
  edit <sensor_str>
    set comment <comment_str>
    set dlp-log {disable | enable}
    set nac-quar-log (disable | enable}
    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
    clone clone <name1> <name2>
  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
`dlp-log {disable | enable}`	Enable or disable logging for data leak protection.	disable
`nac-quar-log (disable | enable}`	Enable or disable logging when data leak protection quarantine’s a user.	disable
`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`
`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`

Variable	**Description**	**Default**
`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`
`clone <name1> <name2>`	Clone an existing DLP sensor. Cloning can be used for upgrading default DLP regular expressions to new improved ones.	

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:

app-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 app-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 | not-installed running | not-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 | not-installed running | not-running}`	Select the condition on which to take action.	`installed`
`vendor <vendor_id>`	Enter the vendor ID. Enter `0` for all vendors. For a list of vendor IDs, enter `set vendor ?`	`0`

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 capability-based-check {enable|disable}
    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 app-detect rule-list" on page 64. This is available if `application-detection` is enabled.	No default.
`capability-based-check {enable|disable}`	Enable to allow non-compliant endpoint access.	`disable`
`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`

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`

firewall

Use firewall commands to configure firewall policies and the data they use.

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.

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 a descriptive comment 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`

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.

carrier-endpoint-bwl

Use FortiOS Carrier carrier end point filtering (also called carrier end point blocking) to control access to MMS services for users according to their carrier end point. Carrier end point filtering can filter MM1, MM3, MM4, and MM7 messages according to the carrier end points in the *From* or *To* addresses of the messages.

Syntax

```
config firewall carrier-endpoint-bwl
  edit <carr-endpnt-lst-integer>
    set comment <carr_endpnt_lst_comment>
  config entries
      edit <carr_endpnt_pattern>
        set pattern-type {regexp | wildcard | simple}
        set action {none | block | exempt-mass-MMS | exempt }
        set log-action {archive | intercept}
        set status {enable | disable}
      next
    set name <carr_endpnt_lst_name>
  next
end
```

Variable	Description	Default
`action {none	block	exempt-mass-MMS	exempt }`	The action (or actions `archive` and `intercept`) to take if the carrier end point expression is found in the list. **none** — no action is taken **block** — message is not delivered to intended recipient, log message in AV LOG as blocked due to carrier end point **exempt-mass-MMS** — no mass MMS scanning performed **exempt** — exempt user messages from all scanning	`block`
`log-action {archive	intercept}`	`archive` — Message is delivered to intended recipient, MMS transaction is forwarded to FortiAnalyzer archive, an entry is generated in content summary for FortiGate unit. `intercept` — Message is delivered to intended recipient, files are quarantined based on quarantine configuration, log message in AV LOG as intercepted due to carrier end point.	No default
`<carr_endpnt_lst_comment>`	Optional description of the carrier end point filter list. The comment text must be less than 63 characters long, or it will be truncated. Spaces are replaced with a plus sign (+).	`null`
`<carr_endpnt_pattern>`	The carrier end point pattern to use for filtering/searching.	No default
`<carr-endpnt-lst-integer>`	A unique number to identify the carrier end point filter list.	No default
`name <carr_endpnt_lst_name>`	The name of the carrier end point filter list.	`null`
`pattern-type {regexp	wildcard	simple}`	Set the pattern type for the banned word. Choose from `regexp`, `wildcard`., or `simple`. Create patterns for banned carrier end point expressions using Perl regular expressions or wildcards.	`wildcard`
`status {enable	disable}`	Enable carrier end point filter search for carrier end point expression in `carr-endpnt-expression`.	`disable`

carrier-endpoint-ip-filter

In mobile networks, neither the user name nor the IP address can be used to identify a specific user. The only element unique to a user is the carrier end point. The carrier end point IP filter provides a mechanism to block network access for a specific list of carrier end points.

The carrier end point IP filter feature uses a carrier end point filter list created using the CLI command config firewall carrier-endpoint-bwl. To set up a carrier end point IP filter, you must create the carrier end point filter list prior to enabling the carrier end point IP filter feature.

Syntax

```
config firewall carrier-endpoint-ip-filter
  edit <carr_endpnt>
    set log-status {enable | disable}
    set status {enable | disable}
  next
end
```

Variable	Description	Default
`<carr_endpnt>`	The carrier end point to be blocked.	No default
`log-status {enable | disable}`	Enable or disable writing a log message when the carrier end point is blocked.	`disable`
`status {enable | disable}`	Enable or disable blocking the carrier end point.	`disable`

central NAT

Central NAT command allows creating NAT rules, as well as NAT mappings that are set up by the global firewall table. Multiple NAT rules can be added on a FortiGate nd these NAT rules can be used in firewall policies.

A Typical NAT rule consists of:

- source ip address
- original port number
- translated ip address
- translated port number

IP addresses can be single address or multiple addresses that are predefined with an ip pool. Similarly, port numbers can also be a single port or a range of ports.

Syntax

```
config firewall central-nat
  edit <name_str>
    set status {enable | disable}
    set orig-addr <name_ip>
    set nat-ippool <name_ip>
    set orig-port <port_int>
    set nat-port <port_int-port_int>
  end
end
```

Variable	Description	Default
`status {enable | disable}`	Enable or disable central NAT rule	`enable`
`orig-addr <name_ip>`	Enter source ip address name	
`nat-ippool <name_ip>`	Enter translated ip pool name for translated addresses	
`orig-port <port_int>`	Enter port number of the source ip	`0`
`nat-port <port_int-port_int>`	Enter translated port or port range	`0`

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.

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`

gtp

Use this command to configure GTP profiles.

Syntax

```
config firewall gtp
  edit <name_str>
    config apn
      edit index_int
        set action {allow | deny}
        set selection-mode {ms net vrf}
        set value <networkid_str>
      end
    config ie-remove-policy
      edit <index_int>
        set remove-ies {apn-restriction rat-type rai uli imei}
        set sgsn-addr <addr/group_str>
      end
    config imsi
      edit <index_int>
        set action {allow | deny}
        set apn <networkid_str>
        set mcc-mnc <mccmnc_str>
        set selection-mode {ms net vrf}
      end
    config ip-policy
      edit <index_int>
        set action {allow | deny}
        set dstaddr <address_str>
        set srcaddr <address_str>
      end
    config noip-policy
      edit <index_int>
        set action {allow | deny}
        set start <protocol_int>
        set end <protocol_int>
        set type {etsi | ietf}
      end
    config policy
      edit <index_int>
        set action {allow | deny}
        set apn <apn_str>
        set imei <imei_str>
        set imsi <imsi_str>
        set max-apn-restriction {all | private-1 | private-2 | public-1 |
          public-2}
        set messages {create-req create-res update-req update-res}
        set rai <rai_str>
        set rat-type {any geran utran wlan}
        set uli <uli_str>
      end
    set addr-notify <Gi_ipv4>
set apn-filter {enable | disable}
set authorized-sgsns <addr/grp_str>
set context-id <id_int>
set control-plane-message-rate-limit <limit_int>
set create-aa-pdp {allow | deny}
set create-pdp {allow | deny}
set data-record {allow | deny}
set default-apn-action {allow | deny}
set default-imsi-action {allow | deny}
set default-ip-action {allow | deny}
set default-noip-action {allow | deny}
set default-policy-action {allow | deny}
set delete-aa-pdp {allow | deny}
set delete-pdp {allow | deny}
set denied-log {enable | disable}
set echo {allow | deny}
set error-indication {allow | deny}
set extension-log {enable | disable}
set failure-report {allow | deny}
set forwarded-log {enable | disable}
set fwd-relocation {allow | deny}
set fwd-srns-context {allow | deny}
set gtp-in-gtp {allow | deny}
set gtp-pdu {allow | deny}
set handover-group
set identification {allow | deny}
set ie-remover {enable | disable}
set imsi-filter {enable | disable}
set interface-notify <interface_str>
set invalid-reserved-field {allow | deny}
set ip-filter {enable | disable}
set log-freq <drop_int>
set max-message-length <bytes_int>
set min-message-length <bytes_int>
set miss-must-ie {allow | deny}
set node-alive {allow | deny}
set noip-filter {enable | disable}
set note-ms-present {allow | deny}
set out-of-state-ie {allow | deny}
set out-of-state-message {allow | deny}
set pdu-notification {allow | deny}
set policy-filter {enable | disable}
set port-notify <port_int>
set ran-info {allow | deny}
set rate-limited-log {enable | disable}
set redirection {allow | deny}
set relocation-cancel {allow | deny}
set reserved-ie {allow | deny}
set send-route {allow | deny}
set seq-number-validate {enable | disable}
set sgsn-context {allow | deny}
set spoof-src-addr {allow | deny}
set state-invalid-log {enable | disable}
set support-extension {allow | deny}
```

```
        set traffic-count-log {enable | disable}
        set tunnel-limit <limit_int>
        set tunnel-limit-log {enable | disable}
        set tunnel-timeout <time_int>
        set unknown-message-action {allow | deny}
        set update-pdp {allow | deny}
        set version-not-support {allow | deny}
      end
```

Variable	Description	Default
`<name_str>`	Enter the name of this GTP profile.	No default.
`apn` The following commands are the options for `config apn`.		
`index_int`	Enter the unique ID number of the APN filter profile.	No default.
`action {allow | deny}`	Select to allow or deny traffic matching both the APN and Selection Mode specified for this APN filter profile.	`allow`
`selection-mode {ms net vrf}`	Select the selection mode or modes required for the APN. The selection mode indicates where the APN originated and whether the Home Location Register (HLR) has verified the user subscription. • Enter `ms` to specify a mobile station provided APN, subscription not verified. This Selection Mode indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network. • Enter `net` to specify a network-provided APN, subscription not verified. This Selection Mode indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user's subscription to the network. • Enter `vrf` to specify a mobile station or network-provided APN, subscription verified. This Selection Mode indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network.	`ms net vrf`
`value <networkid_str>`	Enter the network ID and operator ID of the APN.	No default.
`ie-remove-policy` The following commands are the `set` options for `config ie-remove-policy`.		
`<index_int>`	Enter the unique ID number of the IE removal policy.	No default.
`remove-ies {apn-restriction rat-type rai uli imei}`	Select the information elements to be removed from messages prior to being forwarding to the HGGSN. Any combination of R6 information elements (RAT, RAI, ULI, IMEI-SV and APN restrictions) may be specified.	`apn-restriction rat-type rai uli imei`
`sgsn-addr <addr/group_str>`	Enter an SGSN address or group the IE removal policy will be applied to.	`all`
`imsi` The following commands are the options for `config imsi`.		
`<index_int>`	Enter the unique ID number of the IMSI filtering policy.	No default.
`action {allow | deny}`	Select to allow or deny traffic matching both the APN and Selection Mode specified for this APN filter profile	`allow`
`apn <networkid_str>`	Enter the network ID and operator ID of the APN.	No default.
`mcc-mnc <mccmnc_str>`	Enter the MCC and MNC.	No default.

Variable	Description	Default
`selection-mode {ms net vrf}`	Select the selection mode or modes. The selection mode indicates where the APN originated and whether the Home Location Register (HLR) has verified the user subscription. • Enter `ms` to specify a mobile station provided APN, subscription not verified. This Selection Mode indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network. • Enter `net` to specify a network-provided APN, subscription not verified. This Selection Mode indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user's subscription to the network. • Enter `vrf` to specify a mobile station or network-provided APN, subscription verified. This Selection Mode indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network.	`ms net vrf`
`ip-policy` The following commands are the options for `config ip-policy`.		
`<index_int>`	Enter the unique ID number of the encapsulated IP traffic filtering policy.	No default.
`action {allow | deny}`	Select to allow or deny traffic matching both the source and destination addresses specified for this APN filter profile	`allow`
`dstaddr <address_str>`	Enter the name of a destination address or address group.	No default.
`srcaddr <address_str>`	Enter the name of a source address or address group.	No default.
`noip-policy` The following commands are the options for `config noip-policy`.		
`<index_int>`	Enter the unique ID number of the encapsulated non-IP traffic filtering policy.	No default.
`action {allow | deny}`	Select to allow or deny traffic matching the message protocol specified for this APN filter profile	`allow`
`start <protocol_int>`	Enter the number of the start protocol. Acceptable rate values range from 0 to 255.	`0`
`end <protocol_int>`	Enter the number of the end protocol. Acceptable rate values range from 0 to 255.	`0`
`type {etsi | ietf}`	Select an ETSI or IETF protocol type.	`etsi`
`policy` The following commands are the options for `config policy`.		
`<index_int>`	Enter the unique ID number of the advanced filtering policy.	No default.
`action {allow | deny}`	Select to allow or deny traffic matching the message attributes specified for this advanced filtering policy	`allow`
`apn <apn_str>`	Enter the APN suffix, if required.	No default.
`imei <imei_str>`	Enter the IMEI (SV) pattern, if required.	No default.
`imsi <imsi_str>`	Enter the IMSI prefix, if required.	No default.
`max-apn-restriction {all | private-1 | private-2 | public-1 | public-2}`	Select the maximum APN restriction.	`all`

Variable	Description	Default
`messages {create-req create-res update-req update-res}`	Enter the type or types of GTP messages.	`create-req`
`rai <rai_str>`	Enter the RAI pattern.	No default.
`rat-type {any geran utran wlan}`	Enter the RAT type or types.	`any`
`uli <uli_str>`	Enter the ULI pattern.	No default.
The following commands are the options for `edit <profile_str>`.		
`addr-notify <Gi_ipv4>`	Enter the IP address of the Gi firewall.	`0.0.0.0`
`apn-filter {enable | disable}`	Select to apply APN filter policies.	`disable`
`authorized-sgsns <addr/grp_str>`	Enter authorized SSGN addresses or groups. Any SSGN groups not specified will not be able to send packets to the GGSN. All firewall addresses and groups defined on the FortiGate unit are available for use with this command.	`all`
`context-id <id_int>`	Enter the security context ID. This ID must match the ID entered on the server Gi firewall.	`696`
`control-plane-message-rate-limit <limit_int>`	Enter the control plane message rate limit. Acceptable rate values range from 0 (no limiting) to 2147483674 packets per second. FortiGate units can limit the packet rate to protect the GSNs from possible Denial of Service (DoS) attacks, such as Border gateway bandwidth saturation or a GTP flood.	0
`create-aa-pdp {allow | deny}`	Select to allow or deny all create AA pdp messages.	`allow`
`create-pdp {allow | deny}`	Select to allow or deny all create pdp messages.	`allow`
`data-record {allow | deny}`	Select to allow or deny all data record messages.	`allow`
`default-apn-action {allow | deny}`	Select to allow or deny any APN that is not explicitly defined with in an APN policy.	`allow`
`default-imsi-action {allow | deny}`	Select to allow or deny any IMSI that is not explicitly defined in an IMSI policy.	`allow`
`default-ip-action {allow | deny}`	Select to allow or deny any encapsulated IP address traffic that is not explicitly defined in an IP policy.	`allow`
`default-noip-action {allow | deny}`	Select to allow or deny any encapsulated non-IP protocol that is not explicitly defined in a non-IP policy.	`allow`
`default-policy-action {allow | deny}`	Select to allow or deny any traffic that is not explicitly defined in an advanced filtering policy.	`allow`
`delete-aa-pdp {allow | deny}`	Select to allow or deny all delete AA pdp messages.	`allow`
`delete-pdp {allow | deny}`	Select to allow or deny all delete pdp messages.	`allow`
`denied-log {enable | disable}`	Select to log denied GTP packets.	`disable`
`echo {allow | deny}`	Select to allow or deny all echo messages.	`allow`
`error-indication {allow | deny}`	Select to allow or deny all error indication messages.	`allow`

Variable	Description	Default
`extension-log {enable | disable}`	Select to log extended information about GTP packets. When enabled, this additional information will be included in log entries: • IMSI • MSISDN • APN • Selection Mode • SGSN address for signaling • SGSN address for user data • GGSN address for signaling • GGSN address for user data	`disable`
`failure-report {allow | deny}`	Select to allow or deny all failure report messages.	`allow`
`forwarded-log {enable | disable}`	Select to log forwarded GTP packets.	`disable`
`fwd-relocation {allow | deny}`	Select to allow or deny all forward relocation messages.	`allow`
`fwd-srns-context {allow | deny}`	Select to allow or deny all forward SRNS messages.	`allow`
`gtp-in-gtp {allow | deny}`	Select to allow or deny GTP packets that contains another GTP packet in its message body.	`allow`
`gtp-pdu {allow | deny}`	Select to allow or deny all G-PDU messages.	`allow`
`handover-group`	Handover requests will be honored only from the addresses listed in the specified address group. This way, an untrusted GSN cannot highjack a GTP tunnel with a handover request.	
`identification {allow | deny}`	Select to allow or deny all identification messages.	`allow`
`ie-remover {enable | disable}`	Select whether to use information element removal policies.	`disable`
`imsi-filter {enable | disable}`	Select whether to use IMSI filter policies.	`disable`
`interface-notify <interface_str>`	Enter any local interface of the FortiGate unit. The interface IP address will be used to send the “clear session” message.	
`invalid-reserved-field {allow | deny}`	Select to allow or deny GTP packets with invalid reserved fields. Depending on the GTP version, a varying number of header fields are reserved and should contain specific values. If the reserved fields contain incorrect values, the packet will be blocked if this field is set to `deny`.	`deny`
`ip-filter {enable | disable}`	Select whether to use encapsulated IP traffic filtering policies.	`disable`
`log-freq <drop_int>`	Enter the number of messages to drop between logged messages. An overflow of log messages can sometimes occur when logging rate-limited GTP packets exceed their defined threshold. To conserve resources on the syslog server and the FortiGate unit, you can specify that some log messages are dropped. For example, if you want only every twentieth message to be logged, set a logging frequency of 19. This way, 19 messages are skipped and the next logged. Acceptable frequency values range from 0 to 2147483674. When set to ‘0’, no messages are skipped.	`0`
`max-message-length <bytes_int>`	Enter the maximum GTP message size, in bytes, that the FortiGate unit will allows to pass. Acceptable values range from 0 to 2147483674 bytes. When set to ‘0’, the maximum size restriction is disabled.	`1452`

Variable	Description	Default
`min-message-length <bytes_int>`	Enter the minimum GTP message size, in bytes, that the FortiGate unit will allows to pass. Acceptable values range from 0 to 2147483674 bytes. When set to '0', the minimum size restriction is disabled.	`0`
`miss-must-ie {allow | deny}`	Select to allow or deny passage of GTP packets with missing mandatory information elements to the GGSN.	`deny`
`node-alive {allow | deny}`	Select to allow or deny all node alive messages.	`allow`
`noip-filter {enable | disable}`	Enable or disable the configured encapsulated non-IP traffic filtering policies.	`disable`
`note-ms-present {allow | deny}`	Select to allow or deny all note MS GPRS present messages.	`allow`
`out-of-state-ie {allow | deny}`	Select to allow or deny passage of GTP Packets with out of sequence information elements.	`deny`
`out-of-state-message {allow | deny}`	Select to allow or deny out of state messages. The GTP protocol requires a certain state to be kept by both the GGSN and SGSN. Since the GTP has a state, some message types can only be sent when in specific states. Packets that do not make sense in the current state should be filtered or rejected	`deny`
`pdu-notification {allow | deny}`	Select to allow or deny all pdu notification messages.	`allow`
`policy-filter {enable | disable}`	Enable or disable the configured advanced filtering policies.	`disable`
`port-notify <port_int>`	Enter the server firewall's listening port number.	`21123`
`ran-info {allow | deny}`	Select to allow or deny all RAN info relay messages.	`allow`
`rate-limited-log {enable | disable}`	Select to log rate-limited GTP packets.	`disable`
`redirection {allow | deny}`	Select to allow or deny all redirection messages.	`allow`
`relocation-cancel {allow | deny}`	Select to allow or deny all relocation cancel messages.	`allow`
`reserved-ie {allow | deny}`	Select to allow or deny GTP messages with reserved or undefined information elements.	`deny`
`send-route {allow | deny}`	Select to allow or deny all send route messages.	`allow`
`seq-number-validate {enable | disable}`	Enable or disable sequence number validation The GTP packet header contains a sequence number. The receiving GGSN and the sending GGSN use this number to ensure the packets are in sequence. The FortiGate unit can assume this task and save GGSN resources.	`disable`
`sgsn-context {allow | deny}`	Select to allow or deny all SGSN context messages.	`allow`
`spoof-src-addr {allow | deny}`	Select to allow or deny packets containing spoofed MS addresses. As the MS address is negotiated within the PDP Context creation handshake, any packets originating from the MS that contain a different source address will be detected and dropped if this field is set to deny.	`deny`
`state-invalid-log {enable | disable}`	Select to log GTP packets that have failed stateful inspection.	`disable`
`support-extension {allow | deny}`	Select to allow or deny all support extension messages.	`allow`
`traffic-count-log {enable | disable}`	Enable or disable logging the total number of control and user data messages received from and forwarded to the GGSNs and SGSNs the FortiGate unit protects.	`disable`

Variable	Description	Default
`tunnel-limit <limit_int>`	Enter the maximum number of GTP tunnels according to the GSN capacity.	`0`
`tunnel-limit-log {enable | disable}`	Select to log packets dropped because the maximum limit of GTP tunnels for the destination GSN is reached.	`disable`
`tunnel-timeout <time_int>`	Enter a tunnel timeout value, in seconds. By setting a timeout value, you can configure the FortiGate unit to remove hanging tunnels. Acceptable values range from 0 to 2147483674 seconds. When set to '0', the timeout is disabled.	`86400`
`unknown-message-action {allow | deny}`	Select to allow or deny all unknown message types.	`allow`
`update-pdp {allow | deny}`	Select to allow or deny all update pdp messages.	`allow`
`version-not-support {allow | deny}`	Select to allow or deny all version not supported messages.	`allow`

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`

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`

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 87. To enable or disable IP/MAC binding for an individual FortiGate unit network interface, see `ipmac` in "system interface" on page 381.

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 87.

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`

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 86. To enable or disable IP/MAC binding for an individual FortiGate unit network interface, see `ipmac` in “system interface” on page 381.

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`

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 FortiOS 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

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 137.

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.

mms-profile

Use this command to configure MMS profiles.

Syntax

```
config firewall mms-profile
  edit <profile_str>
    set avnotificationtable <index_int>
    set bwordtable <index_int>
    set carrier-endpoint-prefix {enable | disable}
    set carrier-endpoint-prefix-range-min <limit_int>
    set carrier-endpoint-prefix-range-max <limit_int>
    set carrier-endpoint-prefix-string <prefix_str>
    set carrierendpointbwltable <index_int>
    set comment <str>
    set exmwordtable <index_int>
    set filepattable <index_int>
    set mm1 {archive-full archive-summary avmonitor avquery bannedword block
       carrier-endpoint-bwl chunkedbypass clientcomfort exemptword
       no-content-summary oversize remove-blocked scan server-comfort
       strict-file}
    set mm1-addr-hdr <identifier_str>
    set mm1-addr-source {cookie | http-header}
    set mm1-convert-hex {enable | disable}
    set mm1-retr-dupe {enable | disable}
    set mm1-retrieve-scan {enable | disable}
    set mm1comfortamount <size_int>
    set mm1comfortinterval <seconds_int>
    set mm3 {archive-full archive-summary avmonitor avquery bannedword block
       carrier-endpoint-bwl fragmail no-content-summary oversize remove-
       blocked scan servercomfort splice}
    set mm4 {archive-full archive-summary avmonitor avquery bannedword block
       carrier-endpoint-bwl fragmail no-content-summary oversize remove-
       blocked scan servercomfort splice}
    set mm7 {archive-full archive-summary avmonitor avquery bannedword block
       carrier-endpoint-bwl chunkedbypass clientcomfort exemptword
       no-content-summary oversize remove-blocked scan server-comfort
       strict-file}
    set mm1oversizelimit <limit_int>
    set mm3oversizelimit <limit_int>
    set mm4oversizelimit <limit_int>
    set mm7-addr-hdr <identifier_str>
    set mm7-addr-source {cookie | http-header}
    set mm7-convert-hex {enable | disable}
    set mm7comfortamount <size_int>
    set mm7comfortinterval <seconds_int>
    set mm7oversizelimit <limit_int>
    set mmsbwordthreshold <score_int>
    config dupe {mm1 | mm4}
      set action1 {alert-notif archive archive-first block intercept log}
      set block-time1 <minutes_int>
      set limit1 <duplicatetrigger_int>
      get protocol1
      set status1 {enable | disable}
      set status2 {enable | disable}
      set window1 <minutes_int>
    end
    config flood {mm1 | mm4}
      set action1 {alert-notif archive archive-first block intercept log}
      set block-time1 <minutes_int>
      set limit1 <floodtrigger_int>
      set status1 {enable | disable}
      set status2
      get protocol1
      set window1 <minutes_int>
    end
    config log
      set log-antispam-mass-mms {enable | disable}
      set log-av-block {enable | disable}
      set log-av-carrier-endpoint-filter {enable | disable}
      set log-av-oversize {enable | disable}
      set log-av-virus {enable | disable}
      set log-intercept {enable | disable}
      set log-mms-notification {enable | disable}
      set log-web-content {enable | disable}
    end
    config notification {alert-dupe-1 | alert-flood-1 | mm1 | mm3 | mm4 |
       mm7}
      set alert-int <int>
      set alert-int-mode {minutes | hours}
      set alert-src-msisdn <str>
      set alert-status {enable | disable}
      set bword-int <noticeinterval_int>
      set bword-int-mode {minutes | hours}
      set bword-status {enable | disable}
      set carrier-endpoint-bwl-int <interval_int>
      set carrier-endpoint-bwl-int-mode {hours | minutes}
      set carrier-endpoint-bwl-status {enable | disable}
      set days-allowed {monday tuesday wednesday thursday friday saturday
         sunday}
      set detect-server {enable | disable}
      set dupe-int <interval_int>
      set dupe-int-mode {hours | minutes}
      set dupe-status {enable | disable}
      set file-block-int <interval_int>
      set file-block-int-mode {hours | minutes}
      set file-block-status {enable | disable}
      set flood-int <interval_int>
      set flood-int-mode {hours | minutes}
      set flood-status {enable | disable}
      set from-in-header {enable | disable}
      set mmsc-hostname {<fqdn_str> | <ipv4>}
      set mmsc-password <passwd_str>
      set mmsc-port <port_int>
      set mmsc-url <url_str>
      set mmsc-username <user_str>
      set msg-protocol {mm1 | mm3 | mm4 | mm7}
```

```
      set msg-type {deliver-req | send-req}
      get protocol
      set rate-limit <limit_int>
      set tod-window-start <window_time>
      set tod-window-duration <window_time>
      set user-domain <fqdn_str>
      set vas-id <vas_str>
      set vasp-id <vasp_str>
      set virus-int <interval_int>
      set virus-int-mode {hours | minutes}
      set virus-status {enable | disable}
    end
    config notif-msisdn
      edit <msisdn_int>
        set threshold {dupe-thresh-1 dupe-thresh-2 dupe-thresh-3
           flood-thresh-1 flood-thresh-2 flood-thresh-3}
    end
end
```

Variable	Description	Default
`<profile_str>`	Enter the name of this MMS profile.	No default.
`avnotificationtable <index_int>`	Enter the ID number of the antivirus notification list to be used for the MMS profile. Antivirus notification tables contain virus names that, when detected, will have the FortiGate unit send a notification message to the administrator. For more information on antivirus notification tables, see “notification” on page 38	No default.
`bwordtable <index_int>`	Enter the ID number of the web content block filter to be used for MMS traffic. The web content block tables can be configured using the `config webfilter bword` command.	No default.
`carrierendpointbwltable <index_int>`	Enter the ID number of the endpoint, such as MSISDN, filtering table to use for MMS traffic with the MMS profile.	No default.
`carrier-endpoint-prefix {enable | disable}`	Select to add the country code to the extracted carrier endpoint, such as MSISDN, for logging and notification purposes. You can limit the number length for the test numbers used for internal monitoring without a country code.	`disable`
`carrier-endpoint-prefix-range-min <limit_int>`	Enter the minimum carrier endpoint prefix length. If this and `endpoint-prefix-range-max` are set to zero (0), length is not limited. This option appears only if `msisdn-prefix` is `enable`.	`0`
`carrier-endpoint-prefix-range-max <limit_int>`	Enter the maximum endpoint prefix length. If this and `endpoint-prefix-range-min` are set to zero (0), length is not limited. This option appears only if `msisdn-prefix` is `enable`.	`0`
`carrier-endpoint-prefix-string <prefix_str>`	Enter the endpoint, such as MSISDN, prefix. This option appears only if `endpoint-prefix` is `enable`.	No default.
`comment <str>`	Enter an optional comment to give additional detail about the MMS profile.	
`exmwordtable <index_int>`	Enter the ID number of the webfilter exempt word list to be used with the MMS profile. The web content exempt tables can be configured using the `config webfilter exmword` command.	No default.
`filepattable <index_int>`	Enter the ID number of the file pattern list to be used with the MMS profile.	0

Variable	Description	Default
`mm1 {archive-full archive-summary avmonitor avquery bannedword block carrier-endpoint-bwl chunkedbypass clientcomfort exemptword no-content-summary oversize remove-blocked scan server-comfort strict-file}`	Select actions, if any, the FortiGate unit will take on MMS messages of the specified protocol. **archive-full** — Content archive both metadata and the MMS message itself. **archive-summary** — Content archive metadata. **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 messages containing content in the banned word list. **block** — Block messages matching the file patterns selected by `mms-file-pat-table`, even if the files do not contain viruses. **carrier-endpoint-bwl** — Enable the black/white list specified with the `carrierendpointbwltable` command. **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. This option only available for the `mm1` and `mm7` commands. **clientcomfort** — Apply client comforting to prevent client timeout. This option is available only for `mm1` and `mm7`. **exemptword** — Exempt words from content blocking. This option only available for the `mm1` and `mm7` commands. **fragmail** — Pass fragmented email messages. Fragmented email messages cannot be scanned for viruses. This option only available for the `mm3` and `mm4` commands. **no-content-summary** — Omit MMS filtering statistics from the dashboard. **oversize** — Block files that are over the file size limit. **remove-blocked** — Remove blocked items from messages. **scan** — Scan files for viruses and worms. **server-comfort** — Apply server comforting and prevent server timeout. This option is available only for `mm1` and `mm7`. **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 recipient, listing the virus name and infected file name. This option is available only for `mm3` and `mm4`. **strict-file** — Perform stricter checking for blocked files as specified in `config antivirus filepattern`. This can prevent circumvention by web sites with elaborate scripting using `.exe` or `.dll` files if those patterns are blocked. This option is available only for `mm1` and `mm7`.	No default.
`mm3 {archive-full archive-summary avmonitor avquery bannedword block carrier-endpoint-bwl fragmail no-content-summary oversize remove-blocked scan servercomfort splice}`		no-content-summary splice
`mm4 {archive-full archive-summary avmonitor avquery bannedword block carrier-endpoint-bwl fragmail no-content-summary oversize remove-blocked scan servercomfort splice}`		splice
`mm7 {archive-full archive-summary avmonitor avquery bannedword block carrier-endpoint-bwl chunkedbypass clientcomfort exemptword no-content-summary oversize remove-blocked scan server-comfort strict-file}`		No default.

Variable	Description	Default

`mm1-addr-hdr <identifier_str>`	Enter the sender address (MSISDN) identifier.
	If `mm1-addr-source` is `http-header`, the address and its identifier in the HTTP request header is in the format of:
	`<Sender Address Identifier>: <MSISDN Value>`
	For example, the HTTP header might contain:
	`x-up-calling-line-id: 6044301297`
	where x-up-calling-line-id would be the Sender Address Identifier.
	If `mm1-addr-source` is `cookie`, the address and its identifier in the HTTP request header's Cookie field is in the format of attribute-value pairs:
	`Cookie: id=<cookie-id>;`
	`<Sender Address Identifier>=<MSISDN Value>`
	For example, the HTTP request headers might contain:
	`Cookie: id=0123jf!a;x-up-calling-line-id=6044301297`
	where `x-up-calling-line-id` would be the sender address identifier.
		`x-up-calling-line-id`

`mm1-addr-source {cookie | http-header}`	Select to extract the sender's address from the HTTP header field or a cookie.	`http-header`
`mm1-convert-hex {enable | disable}`	Select to convert the sender address from ASCII to hexadecimal or from hexadecimal to ASCII. This is required by some applications.	`disable`
`mm1-retr-dupe {enable | disable}`	Select to scan MM1 `mm1-retr` messages for duplicates. By default, `mm1-retr` messages are not scanned for duplicates as they may often be the same without necessarily being bulk or spam. This option is available only if `status` is `enable` for the `config dupe mm1` command.	`disable`
`mm1-retrieve-scan {enable | disable}`	Select to scan message retrieval by MM1. If you select `scan` for all MMS interfaces, messages are scanned while being sent, and so scanning message retrieval by MM1 is redundant. In this case, you can disable MM1 message retrieval scanning to improve performance.	enable
`mm1comfortamount <size_int>`	Enter the number of bytes client comforting sends each interval to show a download is progressing. The interval time is set using `mm1comfortinterval.`	1
`mm1comfortinterval <seconds_int>`	Enter the time in seconds before client comforting starts after a download has begun. It is also the interval between subsequent client comforting sends. The amount of data sent each interval is set using `mm1comfortamount`.	10
`mm1oversizelimit <limit_int>`	Block files in MM1 streams that are over this file size limit in KB.	10240
`mm3oversizelimit <limit_int>`	Block files in MM3 streams that are over this file size limit in KB.	10240
`mm4oversizelimit <limit_int>`	Block files in MM4 streams that are over this file size limit in KB.	10240

Variable	Description	Default

`mm7-addr-hdr <identifier_str>`	Enter the sender address (MSISDN) identifier.
	If `mm7-addr-source` is `http-header`, the address and its identifier in the HTTP request header is in the format of:
	`<Sender Address Identifier>: <MSISDN Value>`
	For example, the HTTP header might contain:
	`x-up-calling-line-id: 6044301297`
	where x-up-calling-line-id would be the Sender Address Identifier.
	If `mm7-addr-source` is `cookie`, the address and its identifier in the HTTP request header's Cookie field is in the format of attribute-value pairs:
	`Cookie: id=<cookie-id>;`
	`<Sender Address Identifier>=<MSISDN Value>`
	For example, the HTTP request headers might contain:
	`Cookie: id=0123jf!a;x-up-calling-line-id=6044301297`
	where `x-up-calling-line-id` would be the sender address identifier.
		`x-up-calling-line-id`

`mm7-addr-source {cookie | http-header}`	Select to extract the sender's address from the HTTP header field or a cookie.	`http-header`
`mm7-convert-hex {enable | disable}`	Select to convert the sender address from ASCII to hexadecimal or from hexadecimal to ASCII. This is required by some applications.	`disable`
`mm7oversizelimit <limit_int>`	Block files in MM7 streams that are over this file size limit in KB.	10240
`mm7comfortamount <size_int>`	Enter the number of bytes client comforting sends each interval to show a download is progressing. The interval time is set using `mm7comfortinterval.`	1
`mm7comfortinterval <seconds_int>`	Enter the time in seconds before client comforting starts after a download has begun. It is also the interval between subsequent client comforting sends. The amount of data sent each interval is set using `mm7comfortamount`.	10
`mmsbwordthreshold <score_int>`	Enter the maximum score an MMS message can have before being blocked. If the combined scores of the content block patterns appearing in an MMS message exceed the threshold value, the message will be blocked.	10
`remove-blocked-const-length {enable | disable}`	Select to preserve the length of the MMS message when removing blocked content, such as viruses.	`disable`

config dupe {mm1 | mm4}

Duplicate MMS messages can result from bulk MMS messages, MMS spam, attacks, or other issues.

You can use the `config dupe` subcommand to detect and act on MMS duplicate messages. Thresholds that define excessive duplicate messages and response actions are both configurable.

You can configure MMS duplicate message detection for MM1 messages using `config dupe mm1` and for MM4 messages using `config dupe mm4`.

There are four threshold settings each for mm1 and mm4. The integer at the end of each command indicates which threshold you are configuring. By default, only the first threshold is available for configuration. Enable status2 to gain access to the second threshold. Then enable status3 to gain access to the third threshold. Finally, enable status 4 to gain access to the fourth threshold. They must be enabled in sequence.

Variable	Description	Default

`action1 {alert-notif archive archive-first block intercept log}`	Select the actions to take, if any, when excessive duplicate messages are detected. To select more than one action, separate each action with a space.
	alert-notif — Enable to have the FortiGate unit send a notification message If this threshold is exceeded.
	archive — Archive duplicates in excess of the configured threshold.
	archive-first — Archive the first duplicate in excess of the configured threshold.
	block — Block and intercept excess duplicates. If block is selected, messages are also intercepted, even if `intercept` is not selected.
	intercept — Intercept excess duplicates.
	log — Log excess duplicates. This option takes effect only if logging is enabled for bulk MMS message detection. See "log-antispam-mass-mms {enable | disable}" on page 99.
	This option appears only if `status` is set to `enable` for the MMS interface.
		`archive`
		`block`
		`intercept`
		`log`

`block-time1 <minutes_int>`	Enter the amount of time in minutes during which the FortiGate unit will perform the `action` after a message flood is detected. This option appears only if `status` is `enable` for the MMS interface.	`100`
`limit1 <duplicatetrigger_int>`	Enter the number of messages which signifies excessive message duplicates if exceeded within the `window`. This option appears only if `status` is `enable` for the MMS interface.	`100`
`protocol1`	The MMS interface that you are configuring. `protocol` can be `mm1` or `mm2` depending on whether you entered `config dupe mm1` or `config dupe mm4`. This variable can be viewed with the `get` command, but cannot be `set`.	.
`status1 {enable | disable}`	Select to detect and act upon duplicate MMS messages.	`disable`
`status2 {enable | disable}`	Enable to gain access to the second set of threshold configuration settings.	`disable`
`window1 <minutes_int>`	Enter the period of time in minutes during which excessive message duplicates will be detected if the `limit` is exceeded. This option appears only if `status` is `enable` for the protocol (MM1 or MM4).	`60`

config flood {mm1 | mm4}

Excessive MMS activity (message floods) can result from bulk MMS messages, MMS spam, attacks, or other issues.

You can use the `config flood` subcommand to detect and act on MMS message floods. Thresholds that define a flood of message activity and response actions are both configurable.

You can configure MMS flood detection for MM1 messages using `config flood mm1` and for MM4 messages using `config flood mm4`.

There are four threshold settings for mm1 and mm4. The integer at the end of each command indicates which threshold you are configuring. By default, only the first threshold is available for configuration. Enable status2 to gain access to the second threshold. Then enable status3 to gain access to the third threshold. Finally, enable status 4 to gain access to the fourth threshold. They must be enabled in sequence.

Variable	Description	Default
`action1 {alert-notif archive archive-first block intercept log}`	Select which actions to take, if any, when excessive message activity is detected. To select more than one action, separate each action with a space. **alert-notif** — Enable to have the FortiGate unit send a notification message If this threshold is exceeded. **archive** — Archive messages in excess of the configured threshold. **archive-first** — Archive the first message in excess of the configured threshold. **block** — Block and intercept excess messages. If block is selected, messages are also intercepted, even if `intercept` is not selected. **intercept** — Intercept excess messages. **log** — Log excess messages. This option takes effect only if logging is enabled for bulk MMS message detection. See "log-antispam-mass-mms {enable | disable}" on page 99. This option appears only if `status` is `enable` for the MMS interface.	`block intercept log`
`block-time1 <minutes_int>`	Enter the amount of time in minutes during which the FortiGate unit will perform the `action` after a message flood is detected. This option appears only if `status` is `enable` for the MMS interface.	`100`
`limit1 <floodtrigger_int>`	Enter the number of messages which signifies excessive message activity if exceeded within the `window`. This option appears only if `status` is `enable` for the MMS interface.	`100`
`protocol1`	The MMS interface that you are configuring. `protocol` can be `mm1` or `mm2` depending on whether you entered `config flood mm1` or `config flood mm4`. This variable can be viewed with the `get` command, but cannot be `set`.	
`status1 {enable | disable}`	Select to detect and act upon excessive MMS message activity.	`disable`
`status2 {enable | disable}`	Enable to gain access to the second threshold configuration settings.	`disable`
`window1 <minutes_int>`	Enter the period of time in minutes during which excessive message activity will be detected if the `limit` is exceeded. This option appears only if `status` is `enable` for the MMS interface.	`60`

config log

Use this command to write event log messages when the options that you have enabled in this MMS 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.

All of the `config log` fields are the same as the corresponding `config policy` fields except the following

Variable	Description	Default
`log-antispam-mass-mms {enable | disable}`	Enable to log duplicate or flood MMS notification messages. Also select the `log` action for each protocol and bulk MMS message event that you want to log. For details, see "action1 {alert-notif archive archive-first block intercept log}" on page 97 and "action1 {alert-notif archive archive-first block intercept log}" on page 97.	disable
`log-av-block {enable | disable}`	Enable to log blocked viruses and files.	disable
`log-av-carrier-endpoint-filter {enable | disable}`	Enable to log endpoint, such as MSISDN, blocking, intercepts, and archiving in MMS messages.	disable
`log-av-oversize {enable | disable}`	Enable to log oversized messages.	disable
`log-av-virus {enable | disable}`	Enable to log detected viruses.	disable
`log-intercept {enable | disable}`	Enable to log MMS `intercept` actions in MMS messages.	disable
`log-mms-notification {enable | disable}`	Enable to log MMS notification messages in MMS messages.	disable
`log-web-content {enable | disable}`	Enable to log blocked web content.	disable

config notification {alert-dupe-1 | alert-flood-1 | mm1 | mm3 | mm4 | mm7}

Use this command to configure how the FortiGate unit sends MMS messages to MMS clients to inform them that messages have been sent from their device that violate the settings in this MMS profile. To enable sending notifications you need to enable notification types. You can enable all notification types or you can enable separate notifications for web content blocking, file blocking, end point blocking, flooding, duplicate messages, and virus scanning. You can also use the MMS notifications options to configure how the notification messages are sent.

The FortiGate unit sends notification messages immediately for the first event, then at a configurable interval if events continue to occur. If the interval does not coincide with the window of time during which notices may be sent, the FortiGate unit waits and sends the notice in the next available window. Subsequent notices contain a count of the number of events that have occurred since the previous notification.

There are separate notifications for each notification type, including virus events. Virus event notifications include the virus name. Up to three viruses are tracked for each user at a time. If a fourth virus is found, one of the existing tracked viruses is removed.

The notifications are MM1 `m-send-req` messages sent from the FortiGate unit directly to the MMSC for delivery to the client. The host name of the MMSC, the URL to which `m-send-req` messages are sent, and the port must be specified.

Variable	Description	Default
`alert-int <int>`	Enter the interval the FortiGate will use to send alert messages. The integer you enter will be interpreted as hours or minutes depending on how the `alert-int-mode` command is set.	1
`alert-int-mode {minutes | hours}`	Enter `minutes` or `hours`. This setting will determine whether the integer entered with the `alert-int` command is interpreted as minutes or hours.	hour

Variable	Description	Default
`alert-src-msisdn <str>`	Enter the address the alert messages will appear to be sent from.	
`alert-status {enable | disable}`	Enable to have the FortiGate unit send alert messages.	enable
`bword-int <noticeinterval_int>`	Enter the banned word notification send interval.	`24`
`bword-int-mode {minutes | hours}`	Select whether the value specified in the `bword-int` command is minutes or hours.	`hours`
`bword-status {enable | disable}`	Select to send notices for banned word events.	`disable`
`carrier-endpoint-bwl-int <interval_int>`	Enter the amount of time between notifications for endpoint black/white list events. Also set `endpoint-bwl-status` to `enable` and select the time unit in `endpoint-bwl-int-mode`.	24
`carrier-endpoint-bwl-int-mode {hours | minutes}`	Select the unit of time in minutes or hours for `carrier-endpoint-bwl-int`.	hours
`carrier-endpoint-bwl-status {enable | disable}`	Select to send notices for endpoint black/white list events.	disable
`days-allowed {monday tuesday wednesday thursday friday saturday sunday}`	Notifications will be sent on the selected days of the week.	monday tuesday wednesday thursday friday saturday sunday
`detect-server {enable | disable}`	Select to automatically determine the server address.	`enable`
`dupe-int <interval_int>`	Enter the amount of time between notifications of excessive MMS duplicates. Also set `dupe-status` to `enable` and select the time unit in `dupe-int-mode`.	24
`dupe-int-mode {hours | minutes}`	Select the unit of time in minutes or hours for `dupe-int`. Available only for MM1 and MM4 notifications.	hours
`dupe-status {enable | disable}`	Select to send notices for excessive MMS message duplicate events. Available only for MM1 and MM4 notifications. Available only for MM1 and MM4 notifications.	disable
`file-block-int <interval_int>`	Enter the amount of time between notifications of file block events. Also set `file-block-status` to `enable` and select the time unit in `file-block-int-mode`.	`24`
`file-block-int-mode {hours | minutes}`	Select whether the value specified in the `file-block-int` command is minutes or hours.	`hours`
`file-block-status {enable | disable}`	Select to send notices for file block events.	`disable`
`flood-int <interval_int>`	Enter the amount of time between notifications of excessive MMS activity. Also set `flood-status` to `enable` and select the time unit in `flood-int-mode`. Available only for MM1 and MM4 notifications.	24
`flood-int-mode {hours | minutes}`	Select the unit of time in minutes or hours for `flood-int`. Available only for MM1 and MM4 notifications.	hours
`flood-status {enable | disable}`	Select to send notices for excessive MMS message activity events. Available only for MM1 and MM4 notifications.	disable
`from-in-header {enable | disable}`	Select to insert the “from” address in the HTTP header.	`disable`

Variable	Description	Default
`mmsc-hostname {<fqdn_str> | <ipv4>}`	Enter the FQDN or the IP address of the destination server.	No default.
`mmsc-password <passwd_str>`	Enter the password required for sending messages using this server. (Optional)	No default.
`mmsc-port <port_int>`	Enter the port number the server is using.	Varies by `msg-protocol`.
`mmsc-url <url_str>`	Enter the URL address of the server.	No default.
`mmsc-username <user_str>`	Enter the user-name required for sending messages using this server. (Optional)	No default.
`msg-protocol {mm1 | mm3 | mm4 | mm7}`	Select the protocol to use for sending notification messages.	Depends on `protocol {mm1 | mm3 | mm4 | mm7}`.
`msg-type {deliver-req | send-req}`	Select the type of notification message directed to either a VASP or a MMSC.	deliver-req
`protocol`	The MMS interface that you are configuring. `protocol` can be `mm1`, `mm3`, `mm4` or `mm7` depending on the message type that you are configuring notifications for. This variable can be viewed with the `get` command, but cannot be `set`.	
`rate-limit <limit_int>`	Enter the number of notifications to send per second. If you enter zero (0), the notification rate is not limited.	0
`tod-window-start <window_time>`	Select the time of day to begin sending notifications. If you select a start and end time of zero (`00:00`), notifications are not limited by time of day.	00:00
`tod-window-duration <window_time>`	Select the duration of the period during which the FortiGate unit will send notification messages. If you select a start and duration time of zero (`00:00`), notifications are not limited by time of day.	00:00
`user-domain <fqdn_str>`	Enter the FQDN of the server to which the user's address belongs.	No default.
`vas-id <vas_str>`	Enter the value added service (VAS) ID to be used when sending a notification message. This option is available only when `msg-type` is set to `send-req`.	No default.
`vasp-id <vasp_str>`	Enter the value added service provider (VASP) ID to be used when sending a notification message. This option is available only when `msg-type` is set to `send-req`.	No default.
`virus-int <interval_int>`	Enter the amount of time between notifications for antivirus events. Also set `virus-status` to `enable` and select the time unit in `virus-int-mode`.	`24`
`virus-int-mode {hours | minutes}`	Select the unit of time in minutes or hours for `virus-int`.	`hours`
`virus-status {enable | disable}`	Select to send notices for antivirus events.	`disable`

Example

This example shows how to enable sending MMS notifications for all MM3 notification types and set the interval for each one to 400 minutes:

```
config firewall mms-profile
  edit example
    config notification mm3
```

```
        set bword-status enable
        set bword-int-mode minutes
        set bword-int 400
        set file-block-status enable
        set file-block-mode minutes
        set file-block-int 400
        set carrier-endpoint-bwl-status enable
        set carrier-endpoint-bwl-int-mode minutes
        set carrier-endpoint-bwl-int 400
        set virus-status enable
        set virus-int-mode minutes
        set virus-int 400
      end
    end
```

config notif-msisdn

Individual MSISDN users can be configured to have specific duplicate and flood thresholds.

Variable	Description	Default
`<msisdn_int>`	Enter the MSISDN number. Enter a new number to create a new entry.	
`threshold {dupe-thresh-1 dupe-thresh-2 dupe-thresh-3 flood-thresh-1 flood-thresh-2 flood-thresh-3}`	Enter the thresholds on which this MSISDN user will receive an alert. Clear all thresholds with the `unset threshold` command.	(null)

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 452 and tp-mc-skip-policy {enable | disable} in “system global” on page 364.

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`

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-method {basic | digest | fsae | ntlm}
    set auth-path {enable | disable}
    set auth-redirect-addr <domainname_str>
    set comments <comment_str>
    set custom-log-fields <fieldid_int>
    set dponly {disable | enable}
    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-server-for-ntlm <server_str>
    set gtp_profile <name_str>
    set identity-based {enable | disable}
    set inbound {enable | disable}
    set ip-based {enable | disable}
    set ippool {enable | disable}
    set logtraffic {enable | disable}
    set log-unmatched-traffic {disable | enable}
    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 redirect-url <name_str>
    set rtp-nat {disable | enable}
    set rtp-addr <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 tcp-reset {enable | disable}
    set traffic-shaper <name_str>
    set traffic-shaper-reverse <name_str>
    set per-ip-shaper <name_str>
    set vpntunnel <name_str>
    set wccp {enable | disable}
    set utm-status {disable | enable}
    set profile-type {group | single}
    set profile-group {group | single}
    set profile-protocol-options <name_str>
    set av-profile <name_str>
    set webfilter-profile <name_str>
    set spamfilter-profile <name_str>
    set ips-sensor <name_str>
    set dlp-sensor <name_str>
    set application-list <name_str>
    set voip-profile <name_str>
    set mms-profile <name_str>
    set replacemsg-group <name_str>
    config identity-based-policy
      edit <policy_id>
        set groups <group_name>
        set logtraffic {enable | disable}
        set schedule <name_str>
        set service <name_str>
        set traffic-shaper <name_str>
        set traffic-shaper-reverse <name_str>
        set per-ip-shaper <name_str>
        set utm-status {disable | enable}
        set profile-type {group | single}
        set profile-group {group | single}
        set profile-protocol-options <name_str>
        set av-profile <name_str>
        set webfilter-profile <name_str>
        set spamfilter-profile <name_str>
        set ips-sensor <name_str>
        set dlp-sensor <name_str>
        set application-list <name_str>
        set voip-profile <name_str>
        set mms-profile <name_str>
        set replacemsg-group <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.
`auth-method {basic | digest | fsae | ntlm}`	If `srcintf` is `web-proxy and identity-based` is enabled, select the authentication method. `fsae` is available only if `ip-based` is enabled.	`basic`
`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 215. 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 454.	`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 44.	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 174.	No default.

Variable	Description	Default
`dponly {disable | enable}`	For FortiOS Carrier, enable to configure the firewall policy to only accept sessions with source addresses that are in the dynamic profile user context list. Sessions with source addresses that are not in the user context list do not match the policy. For sessions that don't match the policy, the FortiOS Carrier unit continues searching down the policy list for a match.	`disable`
`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.	`disable`
`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. 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 137.	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`

Variable	Description	Default
`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 63.	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 65.	No default.
`fsae {enable | disable}`	Enable or disable Directory Service authentication.	disable
`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.
`gtp_profile <name_str>`	For FortiOS Carrier, enter the name of a profile to add the GTP profile to the policy.	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`
`ip-based {enable | disable}`	If `srcintf` is `web-proxy and identity-based` is enabled, enable `ip-based` to handle FSAE authentication.	`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`
`log-unmatched-traffic {disable | enable}`	Enable or disabling logging dropped traffic for policies with `identity-based` enabled.	`disable`
`match-vip {enable | disable}`	If you want to explicitly drop a packet that is not matched with a firewall policy and write a log message when this happens, you can add a general policy (source and destination address set to ANY) to the bottom of a policy list and configure the firewall policy to DENY packets and record a log message when a packet is dropped. In some cases, when a virtual IP performs destination NAT (DNAT) on a packet, the translated packet may not be accepted by a firewall policy. If this happens, the packet is silently dropped and therefore not matched with the general policy at the bottom of the policy list. To catch these packets, enable `match-vip` in the general policy. Then the DNATed packets that are not matched by a VIP policy are matched with the general policy where they can be explicitly dropped and logged.	`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. 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`

Variable	Description	Default
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. 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.
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 only appears if disclaimer is enable.	No default.
rtp-nat {disable | enable}	Enable to apply source NAT to RTP packets received by the firewall policy. This field is used for redundant SIP configurations. If rtp-nat is enabled you must add one or more firewall addresses to the rtp-addr field.	disable
rtp-addr <name_str>	Enter one or more RTP firewall addresses for the policy. Separate multiple firewall addresses with a space. This field is only available when rtp-nat is enabled.	
schedule <name_str>	Enter the name of the one-time or recurring schedule or schedule group to use for the policy.	No 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 551.	No default.

Variable	Description	Default
`srcintf <name_str>`	Enter the source interface for the policy. The interface can be a physical interface, a VLAN subinterface, a zone, or web-proxy. 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.	`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`
`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`
`tcp-reset {enable | disable}`	Perform a TCP Reset on TCP traffic that matches a deny policy.	`disable`
`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.

Variable	Description	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.
per-ip-shaper <name_str>	Select a per-ip 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.
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
utm-status {disable | enable}	Enable or disable UTM for the firewall policy. If you enable UTM you must add one ore more UTM profiles and sensors (or a group profile) to the firewall policy. This option appears only if identity-based is disable.	disable
profile-type {group | single}	Select whether to add individual UTM profiles or a UTM profile group to the firewall policy. This option appears only if identity-based is disable.	single
profile-group {group | single}	Enter the name of a UTM profile group to add to the firewall policy. This option is available if profile-type is set to group. This option appears only if identity-based is disable and utm-status is enable.	(null)
profile-protocol-options <name_str>	Enter the name of the protocol options profile to add to the firewall policy. This option appears only if identity-based is disable and utm-status is enable.	(null)
av-profile <name_str>	Enter the name of the antivirus profile to add to the firewall policy. This option appears only if identity-based is disable and utm-status is enable. To add an av-profile, you must obtain an adequate profile name in profile-protection-options.	(null)
webfilter-profile <name_str>	Enter the name of the web filtering profile to add to the firewall policy. This option appears only if identity-based is disable and utm-status is enable.To add a webfilter-profile, you must obtain an adequate profile name in profile-protection-options.	(null)
spamfilter-profile <name_str>	Enter the name of the email filter profile to add to the firewall policy. This option appears only if identity-based is disable and utm-status is enable. To add a spamfilter-profile, you must obtain an adequate profile name in profile-protection-options.	(null)
ips-sensor <name_str>	Enter the name of the IPS sensor to add to the firewall policy. This option appears only if identity-based is disable and utm-status is enable.	(null)
dlp-sensor <name_str>	Enter the name of the DLP sensor to add to the firewall policy. This option appears only if identity-based is disable and utm-status is enable.	(null)
application-list <name_str>	Enter the name of the application list to add to the firewall policy. This option appears only if identity-based is disable and utm-status is enable.	(null)

Variable	Description	Default
`voip-profile <name_str>`	Enter the name of the VoIP profile to add to the firewall policy. This option appears only if `identity-based` is `disable` and `utm-status` is `enable`.	`(null)`
`mms-profile <name_str>`	For FortiOS Carrier, enter the name of the MMS profile to add to the firewall policy. This option appears only if `identity-based` is `disable` and `utm-status` is `enable`.	`(null)`
`replacemsg-group <name_str>`	For FortiOS Carrier, enter the name of the replacement message group to add to the firewall policy. This option appears only if `identity-based` is `disable` and `utm-status` is `enable.`	`default`

config identity-based-policy

Create an identity-based firewall policy that requires authentication. This option is only available if `identity-based` is `enabled`.

Variable	Description	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
`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.
`per-ip-shaper <name_str>`	Enter the per-IP traffic shaper for the identity-based policy.	No default.
`utm-status {disable | enable}`	Enable or disable UTM for the identity-based policy. If you enable UTM you must add one ore more UTM profiles and sensors (or a profile group) to the identify-based policy.	`disable`
`profile-type {group | single}`	Select whether to add individual UTM profiles or a UTM profile group to the identity-based policy.	`single`
`profile-group {group | single}`	Enter the name of a UTM profile group to add to the identity-based policy. This option is available if `profile-type` is set to `group`.	`(null)`
`profile-protocol-options <name_str>`	Enter the name of the protocol options profile to add to the firewall policy.	`(null)`
`av-profile <name_str>`	Enter the name of the antivirus profile to add to the identify-based policy.	`(null)`
`webfilter-profile <name_str>`	Enter the name of the web filtering profile to add to the identify-based policy.	`(null)`
`spamfilter-profile <name_str>`	Enter the name of the email filter profile to add to the identify-based policy.	`(null)`
`ips-sensor <name_str>`	Enter the name of the IPS sensor to add to the identify-based policy.	`(null)`
`dlp-sensor <name_str>`	Enter the name of the DLP sensor to add to the identify-based policy.To add a `dlp-sensor`, you must obtain an adequate name in `profile-protection-options`.	`(null)`
`application-list <name_str>`	Enter the name of the application list to add to the identify-based policy.	`(null)`

Variable	**Description**	**Default**
`voip-profile <name_str>`	Enter the name of the VoIP profile to add to the identify-based policy.	`(null)`
`mms-profile <name_str>`	For FortiOS Carrier, enter the name of the MMS profile to add to the identify-based policy.	`(null)`
`replacemsg-group <name_str>`	For FortiOS Carrier, enter the name of the replacement message group to add to the identify-based policy.	`default`

profile-group

Use this command in FortiOS Carrier to create profile groups. A profile group can contain an antivirus profile, IPS sensor, web filter profile, email filter profile, DLP sensor, application control list, a VoIP profile, an MMS profile and a replacement message group. Once you create profile groups you can add them to firewall policies instead of adding individual UTM profiles and lists.

Syntax

```
config firewall profile-group
  edit <name_str>
    set profile-protocol-options <name_str>
    set av-profile <name_str>
    set webfilter-profile <name_str>
    set spamfilter-profile <name_str>
    set ips-sensor <name_str>
    set dlp-sensor <name_str>
    set application-chart {top10-app | top10-media-user | top10-p2p-user}
    set application-chart {top10-app | top10-media-user | top10-p2p-user}
    set voip-profile <name_str>
    set mms-profile <name_str>
    set replacemsg-group <name_str>
end
```

Variable	Description	Default
`<name_str>`	Enter the name of the profile group.	
`profile-protocol-options <name_str>`	Enter the name of the protocol options profile to add to the profile group.	`(null)`
`av-profile <name_str>`	Enter the name of the antivirus profile to add to the profile group. To add an `av-profile`, you must obtain an adequate profile name in `profile-protection-options`.	`(null)`
`webfilter-profile <name_str>`	Enter the name of the web filtering profile to add to the profile group. To add a `webfilter-profile`, you must obtain an adequate profile name in `profile-protection-options`.	`(null)`
`spamfilter-profile <name_str>`	Enter the name of the email filter profile to add to the profile group. To add a `spamfilter-profile`, you must obtain an adequate profile name in `profile-protection-options`.	`(null)`
`ips-sensor <name_str>`	Enter the name of the IPS sensor to add to the profile group.	`(null)`
`dlp-sensor <name_str>`	Enter the name of the DLP sensor to add to the profile group.To add an `dlp-sensor`, you must obtain an adequate profile name in `profile-protection-options`.	`(null)`
`application-chart {top10-app | top10-media-user | top10-p2p-user}`	Enter the application chart type. • `top10-app`: Top 10 applications chart • `top10-media-user`: Top 10 media users chart • `top10-p2p-user`: Top 10 P2P users chart	`(null)`
`application-list <name_str>`	Enter the name of the application list to add to the profile group.	`(null)`
`voip-profile <name_str>`	Enter the name of the VoIP profile to add to the profile group.	`(null)`
`mms-profile <name_str>`	For FortiOS Carrier, enter the name of the MMS profile to add to the profile group.	`(null)`
`replacemsg-group <name_str>`	For FortiOS Carrier, enter the name of the replacement message group to add to the profile group.	`default`

profile-protocol-options

Use this command to configure UTM protocol options profiles for firewall policies. Protocol options configure how UTM functionality identifies content protocols such as HTTP, FTP, SMTP, etc.Every firewall policy that includes UTM profiles must include a protcol.options profile.

Syntax

```
config firewall profile-protocol-options
  edit <name_str>
    set comment <comment_str>
    set oversize-log {disable | enable}
    set ssl-invalid-server-cert-log {disable | enable}
    set intercept-log {enable | disable}
      config http
        set port <port_number_int>
        set inspect-all {disable | enable}
        set options {chunkedbypass | clientcomfort | no-content-summary |
            oversize | servercomfort}
        set comfort-interval <interval_int>
        set comfort-amount <amount_int>
        set post-lang <charset1> [<charset2>... <charset5>]
        set oversize-limit <size_int>
        set retry-count <retry_int>
      config https
        set port <port_number_int>
        set options {allow-invalid-server-cert | no-content-summary}
        set oversize-limit <size_int>
      config ftp
        set port <port_number_int>
        set inspect-all {disable | enable}
        set options {clientcomfort | no-content-summary | oversize | splice}
        set comfort-interval <interval_int>
        set comfort-amount <amount_int>
        set oversize-limit <size_int>
      config imap
        set port <port_number_int>
        set inspect-all {disable | enable}
        set options {fragmail | no-content-summary | oversize}
        set oversize-limit <size_int>
      config imaps
        set port <port_number_int>
        set options {allow-invalid-server-cert | fragmail |
            no-content-summary | oversize}
        set oversize-limit <size_int>
      config pop3
        set port <port_number_int>
        set inspect-all {disable | enable}
        set options {fragmail | no-content-summary | oversize}
        set oversize-limit <size_int>
      config pop3s
        set port <port_number_int>
        set options {allow-invalid-server-cert | fragmail |
            no-content-summary | oversize}
        set oversize-limit <size_int>
      config smtp
        set port <port_number_int>
        set inspect-all {disable | enable}
        set options {fragmail | no-content-summary | oversize | splice}
        set oversize-limit <size_int>
        set server_busy {disable | enable}
      config smtps
        set port <port_number_int>
        set fragmail no-content-summary
        set options {fragmail | no-content-summary | oversize | splice}
        set oversize-limit <size_int>
      config nntp
        set port <port_number_int>
        set inspect-all {disable | enable}
        set options { no-content-summary | oversize | splice}
        set oversize-limit <size_int>
      config im
        set options { no-content-summary | oversize}
        set oversize-limit <size_int>
      config mail-signature
        set status {disable | enable}
        set signature <text>
  end
```

Variable	Description	Default
`<name_str>`	Enter the name of the protocol options profile.	
`comment <comment_str>`	Optionally enter a description of up to 63 characters of the protocol options profile.	
`oversize-log {disable | enable}`	Enable or disable logging for antivirus oversize file blocking.	`disable`
`ssl-invalid-server-cert-log {disable | enable}`	Enable or disable logging for SSL server certificate validation.	`disable`
`intercept-log {enable | disable}`	Enable or disable logging for FortiOS Carrier antivirus file filter is set to `intercept`.	

config http

Configure HTTP protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for HTTP content.	`80`
`inspect-all {disable | enable}`	Enable to monitor all ports for the HTTP protocol. If you enable this option you can't select a port.	`disable`

Variable	Description	Default
options {chunkedbypass | clientcomfort | no-content-summary | oversize | servercomfort}	Select one or more options apply to HTTP sessions. To select more than one, enter the option names separated by a space. 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. no-content-summary do not add content information from the dashboard. oversize block files that are over the file size limit. servercomfort apply server comforting and prevent server timeout.	no-content-summary
comfort-interval <interval_int>	Enter the time in seconds to wait before client comforting starts after a download has begun. It is also the interval between subsequent client comforting sends. The range is 1 to 900 seconds.	10
comfort-amount <amount_int>	Enter the number of bytes client comforting sends each interval to show that an HTTP download is progressing. The range is 1 to 10240 bytes.	1
post-lang <charset1> [<charset2>... <charset5>]	For HTTPS post pages, because character sets are not always accurately indicated in HTTPS posts, you can use this option to specify up to five character set encodings. The FortiGate unit performs a forced conversion of HTTPS 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.	
oversize-limit <size_int>	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the oversize-limit, the file is passed or blocked, depending on whether oversize is a selected HTTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	10
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

config https

Configure HTTPS protocol options.

Variable	Description	Default
port <port_number_int>	Enter the port number to scan for HTTPS content.	443
options {allow-invalid-server-cert | no-content-summary}	Select one or more options apply to HTTPS sessions. To select more than one, enter the option names separated by a space. allow-invalid-server-cert allow SSL sessions even if server certificate validation failed for the session. no-content-summary do not add content information from the dashboard.	no-content-summary
oversize-limit <size_int>	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the oversize-limit, the file is passed or blocked. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	10

Variable	Description	Default
`post-lang <charset1> [<charset2>... <charset5>]`	For HTTP post pages, because character sets are not always accurately indicated in HTTP posts, you can use this 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.	
`deep-scan {disable | enable}`	Enable to decrypt HTTPS traffic and perform additional scanning of the content of the HTTPS traffic. Using this option requires adding HTTPS server certificates to the FortiGate unit so that HTTPS traffic can be unencrypted.	`disable`

config ftp

Configure FTP protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for FTP content.	`21`
`inspect-all {disable | enable}`	Enable to monitor all ports for the FTP protocol. If you enable this option you can’t select a port.	`disable`
`options {clientcomfort | no-content-summary | oversize | splice}`	Select one or more options apply to FTP sessions. To select more than one, enter the option names separated by a space. `clientcomfort` apply client comforting and prevent client timeout. `no-content-summary` do not add content information from the dashboard. `oversize` block files that are over the file size limit. `splice` simultaneously scan a file and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection.	`no-content-summary splice`
`comfort-interval <interval_int>`	Enter the time in seconds to wait before client comforting starts after a download has begun. It is also the interval between subsequent client comforting sends. The range is 1 to 900 seconds.	`10`
`comfort-amount <amount_int>`	Enter the number of bytes client comforting sends each interval to show that an FTP download is progressing. The range is 1 to 10240 bytes.	`1`
`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected FTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit’s RAM.	`10`

config imap

Configure IMAP protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for IMAP content.	`143`
`inspect-all {disable | enable}`	Enable to monitor all ports for the IMAP protocol. If you enable this option you can’t select a port.	`disable`

Variable	Description	Default
`options {fragmail | no-content-summary | oversize}`	Select one or more options apply to IMAP sessions. To select more than one, enter the option names separated by a space. `fragmail` allow fragmented email. Fragmented email cannot be scanned for viruses. `no-content-summary` do not add content information from the dashboard. `oversize` block files that are over the file size limit.	`fragmail` `no-content-summary`
`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected IMAP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`

config imaps

Configure secure IMAP (IMAPS) protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for IMAPS content.	`993`
`options {allow-invalid-server-cert | fragmail | no-content-summary | oversize}`	Select one or more options apply to IMAPS sessions. To select more than one, enter the option names separated by a space. `allow-invalid-server-cert` allow SSL sessions even if server certificate validation failed for the session. `fragmail` allow fragmented email. Fragmented email cannot be scanned for viruses. `no-content-summary` do not add content information from the dashboard. `oversize` block files that are over the file size limit.	`fragmail` `no-content-summary`
`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected IMAPS option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`

config pop3

Configure POP3 protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for POP3 content.	`110`
`inspect-all {disable | enable}`	Enable to monitor all ports for the POP3 protocol. If you enable this option you can't select a port.	`disable`
`options {fragmail | no-content-summary | oversize}`	Select one or more options apply to POP3 sessions. To select more than one, enter the option names separated by a space. `fragmail` allow fragmented email. Fragmented email cannot be scanned for viruses. `no-content-summary` do not add content information from the dashboard. `oversize` block files that are over the file size limit.	`fragmail` `no-content-summary`
`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected POP3 option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`

config pop3s

Configure secure POP3 (POP3S) protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for POP3S content.	`995`
`options {allow-invalid-server-cert | fragmail | no-content-summary | oversize}`	Select one or more options apply to POP3S sessions. To select more than one, enter the option names separated by a space. `allow-invalid-server-cert` allow SSL sessions even if server certificate validation failed for the session. `fragmail` allow fragmented email. Fragmented email cannot be scanned for viruses. `no-content-summary` do not add content information from the dashboard. `oversize` block files that are over the file size limit.	`fragmail` `no-content-summary`
`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected POP3 option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`

config smtp

Configure SMTP protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for SMTP content.	`25`
`inspect-all {disable | enable}`	Enable to monitor all ports for the SMTP protocol. If you enable this option you can't select a port.	`disable`

`options {fragmail | no-content-summary | oversize | splice}`	Select one or more options apply to SMTP sessions. To select more than one, enter the option names separated by a space.
	`fragmail` allow fragmented email. Fragmented email cannot be scanned for viruses.
	`no-content-summary` do not add content information from the dashboard.
	`oversize` block files that are over the file size limit.
	`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.
		`fragmail`
		`no-content-summary`
		`splice`

Variable	Description	Default
`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected SMTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`
`server_busy {disable | enable}`	Enable this options so that when the FortiGate unit attempts to send an SMTP email but can't because of a connection timeout or connection error it returns a 412 server busy error message to the email client attempting to send the message. Usually the FortiGate unit accepts SMTP SYN from clients and immediately send back ACK before actually connecting with the real SMTP server. If the server responds back with NACK (service not available) the FortiGate-to-server connection drops, but the FortiGate-to-client connection will just hang until a timeout occurs. This causes particular problems for systems that use alternative servers, they may not move to the next server until the timeout occurs. Not all SMTP mail servers behave in this way, some use an SMTP HELO to confirm the connection is active and so do not have an issue with this behavior.	`disable`

config smtps

Configure secure SMTP (SMTPS) protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for SMTPS content.	`465`
`options {fragmail | no-content-summary | oversize | splice}`	Select one or more options apply to SMTPS sessions. To select more than one, enter the option names separated by a space. `fragmail` allow fragmented email. Fragmented email cannot be scanned for viruses. `no-content-summary` do not add content information from the dashboard. `oversize` block files that are over the file size limit. `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 SMTPS spam. When streaming mode is disabled for SMTP, infected attachments are removed and the email is forwarded (without the attachment) to the SMTPS server for delivery to the recipient. Throughput is higher when streaming mode is enabled.	`fragmail` `no-content-summary`
`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected SMTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`

config nntp

Configure NNTP protocol options.

Variable	Description	Default
`port <port_number_int>`	Enter the port number to scan for NNTP content.	`119`
`inspect-all {disable | enable}`	Enable to monitor all ports for the NNTP protocol. If you enable this option you can't select a port.	`disable`

Variable	Description	Default

`options {`
`no-content-summary |`
`oversize | splice}`
	Select one or more options apply to NNTP sessions. To select more than one, enter the option names separated by a space.
	`no-content-summary` do not add content information from the dashboard.
	`oversize` block files that are over the file size limit.
	`splice` simultaneously scan a file and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection.
		`no-content-summary`

`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected NNTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`

config im

Configure IM protocol options.

Variable	Description	Default

`options {`
`no-content-summary |`
`oversize}`
	Select one or more options apply to IM sessions. To select more than one, enter the option names separated by a space.
	`no-content-summary` do not add content information from the dashboard.
	`oversize` block files that are over the file size limit.
		`no-content-summary`

`oversize-limit <size_int>`	Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the `oversize-limit`, the file is passed or blocked depending on whether `oversize` is a selected IM option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM.	`10`

config mail-signature

Configure email signature options for SMTP.

Variable	Description	Default
`status {disable | enable}`	Enable or disable adding an email signature to SMTP email messages as they pass through the FortiGate unit.	`disable`
`signature <text>`	Enter a signature to add to outgoing email. If the signature contains spaces, surround it with single or double quotes (`‘` or `"`).	`(null)`

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

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`

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.

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 705.

Syntax

```
config firewall service custom
  edit <name_str>
    set comment <string>
    set icmpcode <code_int>
    set icmptype <type_int>
    set protocol {ICMP | ICMP6 | IP | TCP/UDP/SCTP}
    set protocol-number <protocol_int>
    set sctp-portrange <dstportlow_int>[-<dstporthigh_int>:
       <srcportlow_int>-<srcporthigh_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 | ICMP6 | IP | TCP/UDP/SCTP}`	Select the protocol used by the service. If you select `TCP/UDP/SCTP` you must specify the `tcp-portrange`, `udp-portrange`, or `sctp-portrange`.	`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`
`sctp-portrange <dstportlow_int>[-<dstporthigh_int>: <srcportlow_int>-<srcporthigh_int>]`	For SCTP services, enter the destination and source port ranges. If the destination port range can be any port, enter `0-65535`. 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.

Variable	Description	Default
`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 `0-65535`. 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 `0-65535`. 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.

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.

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 max-bandwidth <kBps_int>
    set max-concurrent-session <sessions_int>
end
```

Variable	Description	Default
`<name_str>`	Enter the name of the traffic shaper.	No default.
`max-bandwidth <kBps_int>`	Enter the maximum amount of bandwidth available for an IP address controlled by the policy. `KBps_int` can be 0 to 2097000 KBytes/second. If maximum bandwidth is set to 0 no traffic is allowed by the policy.	`0`
`max-concurrent-session <sessions_int>`	Enter the maximum number of sessions allowed for an IP address. `sessions_int` can be 0 to 2097000. If maximum concurrent sessions is 0 then no sessions are allowed.	`0`

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 guaranteed-bandwidth <bandwidth_value>
    set maximum-bandwidth <bandwidth_value>
    set per-policy {enable | disable}
    set priority {high | low | medium}
  end
end
```

Variable	Description	Default
`<name_str>`	Enter the name of the traffic shaper.	No default.
`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`

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 389 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 mode 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`

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 389 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 mode 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`

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 no-matching-cipher-action {bypass | drop}
  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`
`no-matching-cipher-action {bypass | drop}`	Bypass or drop SSL traffic when unsupported cipher is being used by the server.	`bypass`
`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`

Variable	Description	Default
`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`

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 {sctp | tcp | udp}
        set server-type {http | https | ip | ssl | tcp | udp}
        set ssl-mode {full | half}
        set ssl-certificate <certificate_str>
        set ssl-client-recognition {allow | deny}
        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_ipv4> [<ip_range_ipv4>] [<ip_range_ipv4>]
               [<ip_range_ipv4>]
            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

Variable	Description	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.
`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. 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. 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`.	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`.	
`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`.	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`.	

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`.	`same-ip`
`http-ip-header {enable | disable}`	Select to preserve the client's IP address in the `X-Forwarded-For` HTTP header line if HTTP multiplexing is enabled. This can be useful if you require logging on the server of the client's original IP address. If this option is not selected, in HTTP multiplexing configurations the header will contain the IP address of the FortiGate unit. This option appears only if `portforward` and `http-multiplex` 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`.	`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.

Variable	Description	Default
`nat-source-vip {enable | disable}`	Enable to prevent unintended servers from using a virtual IP. The virtual IP will be used as the source IP address for connections from the server through the FortiGate unit. Disable to use the actual IP address of the server (or the FortiGate destination interface if using NAT) as the source address of connections from the server that pass through the FortiGate unit.	`disable`
`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 142 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 {sctp | 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`.	`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-recognition {allow | deny}`	Enter `allow` to give permission an SSL client to renegotiate or `deny` to abort any SSL connection that attempts to renegotiate. This option appears only if `type` is `server-load-balance` and `server-type` is `ssl`.	`allow`
`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`

Variable	Description	Default
`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`
`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_ipv4> [<ip_range_ipv4>] [<ip_range_ipv4>] [<ip_range_ipv4>]`	Restrict the clients that can connect to a real server according to the client's source IP address. Use the `client-ip` option to enter up to four client source IP addresses or address ranges. Separate each IP address or range with a space. The following example shows how to add a single IP address and an IP address range: `set client-ip 192.168.1.90 192.168.1.100-192.168.1.120` Use the `client-ip` option if you have multiple real servers in a server load balance VIP and you want to control which clients use which real server according to the client's source IP address. Different real servers in the same virtual server can have the same or overlapping IP addresses and ranges. If an overlap occurs, sessions from the overlapping source addresses are load balanced among the real servers with the overlapping addresses. If you do not specify a `client-ip` all clients can use the real server.	
`<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`

Variable	**Description**	**Default**
`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
`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 89. 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 147. • `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

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.

-

gui

This chapter contains the following section:

console

This command stores a base-64 encoded file that contains configuration of the dashboard and *System > Status* web-based manager pages. This command is not user configurable

Syntax

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

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

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

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`

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`

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

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`

- 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`

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

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 381.

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 quarantine-log {enable | disable}
        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.	
`<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
`quarantine-log {enable | disable}`	Enable NAC quarantine logging. NAC quarantine logging is only available when `quarantine` is set something other than `none.`	`disable`
`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

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.

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.

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

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`

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
    set comment <comment_str>
    set log {disable | enable}
    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 log-packet {disable | enable}
        set action {block | default | pass | reject}
        set quarantine {attacker | both | interface | none}
        set quarantine-log {disable | enable}
        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 quarantine-log {disable | enable}
        set status {disable | enable}
      end
  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.	
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.	
log {disable | enable}	Enable or disable IPS logging.	enable
<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
`log-packet {disable | enable}`	When enabled, packet logging will save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use. This feature is only available in FortiGate units with internal hard drives.	`disable`
`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
`quarantine-log {disable | enable}`	Enable or disable writing a log message when a user is quarantined.	

`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.	

Variable	Description	Default
`<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 web-based manager.	
`<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`

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

{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 dlp-archive {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 endpoint-bwl {disable | enable}
  set ftgd-wf-block {disable | enable}
  set ftgd-wf-errors {disable | enable}
  set mass-mms {disable | enable}
  set gtp {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 web-filter-ftgd-quota {disable | enable}
    set web-filter-ftgd-quota-counting {disable | enable}
    set web-filter-ftgd-quota-expired {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`

Variable	Description	Default
`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`
`email-log-smtp {disable | enable}`	Enable or disable logging of spam detected in SMTP traffic. `email enable` only.	`enable`
`endpoint-bwl {disable | enable}`	Enable or disableFortiOS Carrier logging of End-point filter block messages.	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`
`mass-mms {disable | enable}`	Enable or disable FortiOS Carrier logging of a large amount of MMS blocked messages.	`enable`
`gtp {disable | enable}`	Enable or disable FortiOS Carrier logging for GTP messages.	`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 (see “check-protocol-header {loose | strict}” on page 369, “anti-replay {disable | loose | strict}” on page 367, and “check-reset-range {disable | strict}” on page 368. • 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`

Variable	Description	Default
`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`
`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 `traffic` 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`

Variable	Description	Default
`web-filter-ftgd-quota {disable | enable}`	Enable or disable logging FortiGuard quota levels.	`enable`
`web-filter-ftgd-quota-counting {disable | enable}`	Enable or disable logging FortiGuard quota counting messages.	`enable`
`web-filter-ftgd-quota-expired {disable | enable}`	Enable or disable logging FortiGuard quota expired messages.	`enable`
`webcache-traffic {disable | enable}`	Enable or disable WAN optimization web cache traffic logging.	`enable`

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 203:

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 ips-archive {enable | disable}
  set sql-max-size <lsize>
  set sql-max-size-action {overwrite | nolog}
  set storage <name>
  set upload {enable | disable}
  set upload-destination {fortianalyzer | ftp-server}
  set uploadip <class_ip>
  set uploadport <port_integer>
  set source-ip <address_ipv4>
  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 log-quota <integer>
  set dlp-archive-quota <integer>
  set report-quota <integer>
  set ips-packet-quota <integer>
  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`

`ips-archive`
`{enable | disable}`
	Enable IPS packet archive logs.	`enable`

`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`

`storage <name>`	Enter a name for the storage log file. This option is only available when the current vdom is the management vdom.	
`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`

`source-ip`
`<address_ipv4>`
	Enter the source IP address of the disk log uploading.	`0.0.0.0`

Variable	Description	Default
`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

`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`
`log-quota <integer>`	Enter then amount (in MB) of disk space allocated for disk logging.	`0`
`dlp-archive-quota <integer>`	Enter then amount (in MB) of disk space allocated for DLP logs.	`0`
`report-quota <integer>`	Enter then amount (in MB) of disk space allocated for report logs.	`0`
`ips-packet-quota <integer>`	Enter then amount (in MB) of disk space allocated for IPS packet archives.	`0`
`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`

Variable	Description	Default
`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`

eventfilter

Use this command to configure event logging.

Syntax

```
config log eventfilter
  set event {enable | disable}
  set admin {enable | disable}
  set amc-intf-bypass {enable | disable}
  set auth {enable | disable}
  set cpu-memory-usage {enable | disable}
  set dhcp {enable | disable}
  set ha {enable | disable}
  set ipsec {enable | disable}
  set ldb-monitor {enable | disable}
  set nac-quarantine {enable | disable}
  set pattern {enable | disable}
  set ppp {enable | disable}
  set sslvpn-log-adm {enable | disable}
  set sslvpn-log-auth {enable | disable}
  set sslvpn-log-session {enable | disable}
  set system {enable | disable}
  set vip-ssl {enable | disable}
  set voip {enable | disable}
  set wan-opt {enable | disable}
  set wireless-activity {enable | disable}
end
```

Variable	Description	Default
`event {enable | disable}`	Log event messages. Must be enabled to make the following fields available.	`enable`
`admin {enable | disable}`	Log admin login/logout messages.	`enable`
`amc-intf-bypass {enable | disable}`	Log AMC interface entering bypass mode messages.	`enable`
`auth {enable | disable}`	Log firewall authentication messages.	`enable`
`cpu-memory-usage {enable | disable}`	Log CPU & memory usage every 5 minutes.	`disable`
`dhcp {enable | disable}`	Log DHCP service messages.	`enable`
`ha {enable | disable}`	Log HA activity messages.	`enable`
`ipsec {enable | disable}`	Log IPSec negotiation messages.	`enable`
`ldb-monitor {enable | disable}`	Log VIP realserver health monitoring messages.	`enable`
`nac-quarantine {enable | disable}`	Log nac-quarantine messages.	`enable`
`pattern {enable | disable}`	Log pattern update messages.	`enable`
`ppp {enable | disable}`	Log L2TP/PPTP/PPPoE messages.	`enable`
`sslvpn-log-adm {enable | disable}`	Log ssl administration.	`enable`

Variable	Description	Default
`sslvpn-log-auth {enable | disable}`	Log ssl user authentication.	`enable`
`sslvpn-log-session {enable | disable}`	Log ssl session.	`enable`
`system {enable | disable}`	Log system activity messages.	`enable`
`vip-ssl {enable | disable}`	log VIP SSL messages.	`enable`
`voip {enable | disable}`	Log VOIP messages.	`enable`
`wan-opt {enable | disable}`	Log WAN optimization messages.	`enable`
`wireless-activity {enable | disable}`	Log wireless activity.	`enable`

{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 175.

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 188.

{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 `fortianalyzer2` and `fortianalyzer3` 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 status {enable | disable}
  set ips-archive {enable | disable}
  set max-buffer-size <size_int>
  set address-mode {auto-discovery | static}
  set server <fortianalyzer_ipv4>
  set encrypt {enable | disable}
  set psksecret <pre-shared_key>
  set localid <identifier>
  set conn-timeout <seconds>
  set fdp-device <serial_number>
  set fdp-interface <int_str>
end
```

Variable	Description	Default
`status {enable | disable}`	Enable or disable communication with the FortiAnalyzer unit. The other fields are available only if `status` is set to `enable`.	disable
`ips-archive {enable | disable}`	Enable IPS packet archive.	`enable`
`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`
`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`
`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`
`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`
`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
`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.
`source-ip <address_ipv4>`	Enter the source IP address for the FortiAnalyzer, FortiAnalyzer2 and FortiAnalyzer3 units.	`0.0.0.0`
`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
`gui-display {enable | disable}`	Enable to display FortiAnalyzer Reports on the web-based manager.	`disable`

fortiguard setting

Use this command for configuring FortiGuard Analysis Service settings.

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`

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 ips-archive {enable | disable}
  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`
`ips-archive {enable | disable}`	Enable IPS packet archive logs.	`enable`
`status {disable | enable}`	Enter `enable` to enable logging to the FortiGate system memory.	`disable`

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

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 194.

{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 status {disable | enable}
  set server <address_ipv4>
  set reliable {disable | enable}
  set port <port_integer>
  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 source-ip <address_ipv4>
end
```

Variable	Description	Default
`status {disable | enable}`	Enter `enable` to enable logging to a remote syslog server.	`disable`
`server <address_ipv4>`	Enter the IP address of the syslog server that stores the logs.	No default.
`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`
`port <port_integer>`	Enter the port number for communication with the syslog server.	`514`
`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`

Variable	Description	Default
`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`
`source-ip <address_ipv4>`	Enter source IP address for syslogd, syslog2 and syslog3	`0.0.0.0`

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`

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`

netscan

Use these commands to configure the Endpoint network vulnerability scanner.

settings

assets

settings

Use this command to configure network vulnerability scanner settings that control when scans are run.

Syntax

```
config netscan settings
  set scan-mode {full | quick | standard}
  set schedule {disable | enable}
  set day-of-week {monday | tuesday | wednesday | thursday | friday |
     saturday | sunday}
  set day-of-month <day_int>
  set time <hh:mm>
  set recurrence {daily | monthly | weekly}
end
```

Variables	Description	Default
scan-mode {full | quick | standard}	Specify the scan mode to use: full scan all TCP and UDP ports quick perform a quick scan of commonly used TCP and UDP ports standard perform a standard scan of more ports than the quick scan but not all ports.	quick
schedule {disable | enable}	Enable to schedule network vulnerability manager scans. If you disable this option you can only run scans on demand.	disable
day-of-week {monday | tuesday | wednesday | thursday | friday | saturday | sunday}	Select the day of the week on which to run scans. You can only select one day. This option is only available if schedule is enabled and recurrence is weekly.	sunday
day-of-month <day_int>	Enter the day of the month on which to run scans. You can only select one day. This option is only available if schedule is enabled and recurrence is monthly.	1
time <hh:mm>	Enter the time of day on which to start a scan.	00:00
recurrence {daily | monthly | weekly}	Set scheduled scans to run once a day, once a month, or once a week.	weekly

assets

Use this command to define assets (network devices and networks) to run network vulnerability scans on.

Syntax

```
config netscan assets
  edit <asset_id_int>
    set addr-type {ip | range}
    set auth-unix (disable | enable}
    set auth-windows (disable | enable}
    set mode {discovery | scan}
    set name <string>
    set start-ip <address_ipv4>
    set status {disable | enable}
    set end-ip <address_ipv4>
    set unix-password <pass_str>
    set unix-username <id_str>
    set win-password <pass_str>
    set win-username <id_str>
  end
```

Variables	Description	Default
`<asset_id_int>`	Enter the unique ID number for this asset.	
`addr-type {ip | range}`	Select `ip` to scan a single IP address. Select `range` to scan a range of IP addresses.	`ip`
`auth-unix (disable | enable}`	Enable to allow the FortiGate unit to authenticate with a unix host during the vulnerability scan. If you enable this option you must enter a `unix-username` and a `unix-password`.	`disable`
`auth-windows (disable | enable}`	Enable to allow the FortiGate unit to authenticate with a Windows host during the vulnerability scan. If you enable this option you must enter a `win-username` and a `win-password`.	`disable`
`mode {discovery | scan}`	Select `discovery` to find assets with the specified IP address or address range.	`scan`
`name <string>`	Enter an name of the asset.	
`start-ip <address_ipv4>`	Enter the IP address of the asset to scan. If `addr-type` is set to `range` enter the first IP address in the IP address range to scan.	`0.0.0.0`
`status {disable | enable}`	Enable or disable this asset scan configuration.	`enable`
`end-ip <address_ipv4>`	If `addr-type` is set to `range` enter the last IP address in the IP address range to scan.	`0.0.0.0`
`unix-password <pass_str>`	Enter the password the FortiAnalyzer uses to authenticate with the UNIX host. This command appears only when `auth` is set to `unix`.	
`unix-username <id_str>`	Enter the username the FortiAnalyzer uses to authenticate with the UNIX host. This command appears only when `auth` is set to `unix`.	
`win-password <pass_str>`	Enter the password the FortiAnalyzer uses to authenticate with the Windows host.	
`win-username <id_str>`	Enter the username the FortiAnalyzer uses to authenticate with the Windows host.	

report

Use these commands to configure SQL reports. You can use the `get report database schema` to display the FortiGate SQL reporting database schema.

Note: The command descriptions in this chapter have not been updated for FortiOS 4.0 MR2. This chapter will be updated for a future version of this document.

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.	

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`

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.	

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
aspath-list
auth-path
bgp
community-list
isis
key-chain
multicast
ospf
ospf6
policy
prefix-list, prefix-list6
rip
ripng
route-map
setting
static
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 273.

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.

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.`

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.`

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 {disable | enable}
  set fast-external-failover {disable | enable}
  set graceful-restart {disable | enable}
  set graceful-restart-time <restart_time>
  set graceful-stalepath-time <stalepath_time>
  set graceful-update-delay <delay_time>
  set holdtime-timer <seconds_integer>
  set ignore_optional_capability {disable | enable}
  set keepalive-timer <seconds_integer>
  set log-neighbor-changes {disable | enable}
  set network-import-check {disable | enable}
  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 229), and set operating parameters for communicating with BGP neighbors (see “config neighbor” on page 223).

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 290. 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 230) or by using the conditional aggregate routing feature (see “config aggregate-address” on page 223).

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 227), 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`

Variable	Description	Default
`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`
`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 288 and “Using route maps with BGP” on page 290.	`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`

Variable	Description	Default
`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`
`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 {disable | enable}`	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 {disable | enable}`	Immediately reset the session information associated with BGP external peers if the link used to reach them goes down.	`enable`
`graceful-restart {disable | enable}`	Enable or disable BGP support for the graceful restart feature. Graceful restart 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
`graceful-restart-time <restart_time>`	Set the time in seconds needed for neighbors to restart after a graceful restart. The range is 1 to 3600 seconds. Available when `graceful-restart` is enabled.	120
`graceful-stalepath-time <stalepath_time>`	Set the time in seconds to hold stale paths of restarting neighbors. The range is 1 to 3600 seconds. Available when `graceful-restart` is enabled.	360
`graceful-update-delay <delay_time>`	Route advertisement and selection delay in seconds after a graceful restart. The range is 1 to 3600 seconds. Available when `graceful-restart` is enabled.	120
`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 {disable | enable}`	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 {disable | enable}`	Enable or disable the logging of changes to BGP neighbor status.	`disable`
`network-import-check {disable | enable}`	Enable or disable the advertising of the BGP network in IGP (see "config network" on page 229).	`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`

Variable	Description	Default
`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 290) 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`
`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 666).

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
`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`

Variable	Description	Default
`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`
`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 288.	`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 212.	`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 212.	`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 212.	`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 212.	`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`

Variable	Description	Default
`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 214.	`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 214.	`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`
`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 221). 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 221). 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`

Variable	Description	Default
`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`
`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 273.	`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 273.	`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 273.	`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 273.	`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`

Variable	Description	Default
`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 288 and "Using route maps with BGP" on page 290.	`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 288 and "Using route maps with BGP" on page 290.	`Null.`
`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 219). 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`

Variable	Description	Default
`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 288 and "Using route maps with BGP" on page 290.	`Null.`
`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 {disable | enable}`" on page 221) 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 288 and "Using route maps with BGP" on page 290.	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 229).

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.
- isis — Redistribute routes learned from ISIS.
- 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 | isis | 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 288 and "Using route maps with BGP" on page 290. 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
```

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 233.	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.`

isis

IS-IS is described in RFC 1142. You can enable and configure IS-IS on your FortiGate unit if this routing protocol is in use on your network.

Note: For each routing protocol, you can also use a `redistribute` command to redistribute IS-IS routes with the other protocol. For example, to redistribute IS-IS routes over OSFP enter:

```
config router ospf
  config redistribute isis
    set statue enable
  end
end
```

```
config router isis
  set adjacency-check {disable | enable}
  set auth-keychain-l1 <keychain_str>
  set auth-keychain-l2 <keychain_str>
  set auth-mode-l1 {md5 | password}
  set auth-mode-l2 {md5 | password}
  set auth-password-l1 <password>
  set auth-password-l2 <password>
  set auth-sendonly-l1 {disable | enable}
  set auth-sendonly-l2 {disable | enable}
  set default-originate {disable | enable}
  set dynamic-hostname {disable | enable}
  set ignore-lsp-errors {disable | enable}
  set is-type {level-1 | level-1-2 | level-2-only}
  set lsp-gen-interval-l1 <interval_int>
  set lsp-gen-interval-l2 <interval_int>
  set lsp-refresh-interval <interval_int>
  set max-lsp-lifetime <lifetime_int>
  set metric-style {narrow | narrow-transition | narrow-transition-l1 |
     narrow-transition-l2 | transition | transition-l1 | transition-l2 |
     wide | wide-l1 | wide-l2 | wide-transition | wide-transition-l1 | wide-
     transition-l2}
  set overload-bit {disable | enable}
  set overload-bit-on-startup
  set overload-bit-suppress external interlevel
  set redistribute-l1 {disable | enable}
  set redistribute-l1-list <access_list_str>
  set redistribute-l2 {disable | enable}
  set redistribute-l2-list <access_list_str>
  set spf-interval-exp-l1 <minimum_delay_int> <l
  set spf-interval-exp-l2 <min_delay_int> <max_delay_int>
  config isis-interface
    edit <interface_str>
      set auth-keychain-l1 <keychain_str>
      set auth-keychain-l2 <keychain_str>
      set auth-mode-l1 {md5 | password}
      set auth-mode-l2 {md5 | password}
      set auth-password-l1 <password>
      set auth-password-l2 <password>
      set auth-send-only-l1 {disable | enable}
      set auth-send-only-l2 {disable | enable}
      set circuit-type {level-1 | level-1-2 | level-2-only}
      set csnp-interval-l1 <interval_int>
      set csnp-interval-l2 <interval_int>
      set hello-interval-l1 <interval_int>
      set hello-interval-l2 <interval_int>
      set hello-multiplier-l1 <multipler_int>
      set hello-multiplier-l2 <multipler_int>
      set hello-padding {disable | enable}
      set lsp-interval <interval_int>
      set lsp-retransmit-interval <interval_int>
      set mesh-group {disable | enable}
      set mesh-group-id <id_int>
      set metric-l1 <metric_int>
      set metric-l2 <metric_int>
      set network-type {broadcast | point-to-point}
      set priority-l1 <priority_int>
      set priority-l2 <priority_int>
      set status {disable | enable}
      set wide-metric-l1 <metric_int>
      set wide-metric-l2 <metric_int>
  config isis-net
    edit <id>
      set net <user_defined>
  config redistribute {bgp | connected | ospf | rip | static}
    set status {disable | enable}
    set metric <metric_int>
    set metric-type {external | internal}
    set level {level-1 | level-1-2 | level-2}
    set routemap <routmap_name>
  config summary-address
    edit <id>
      set level {level-1 | level-1-2 | level-2}
      set prefix <prefix_ipv4> <prefix_mask>
    end
  end
```

Variable	Description	Default
adjacency-check {disable | enable}	Enable to check neighbor protocol support.	disable
auth-keychain-l1 <keychain_str>	Authentication key-chain for level 1 PDUs. Available when auth-mode-l1 is set to md5.	
auth-keychain-l2 <keychain_str>	Authentication key-chain for level 2 PDUs. Available when auth-mode-l2 is set to md5.	
auth-mode-l1 {md5 | password}	Level 1 authentication mode.	password
auth-mode-l2 {md5 | password}	Level 2 authentication mode.	password
auth-password-l1 <password>	Authentication password for level 1 PDUs. Available when auth-keychain-11 is set to password.	
auth-password-l2 <password>	Authentication password for level 2 PDUs. Available when auth-keychain-12 is set to password.	

Variable	Description	Default
`auth-sendonly-l1 {disable | enable}`	Level 1 authentication send-only.	`disable`
`auth-sendonly-l2 {disable | enable}`	Level 2 authentication send-only.	`disable`
`default-originate {disable | enable}`	Control distribution of default information.	`disable`
`dynamic-hostname {disable | enable}`	Enable dynamic hostname.	`disable`
`ignore-lsp-errors {disable | enable}`	Enable to ignore LSPs with bad checksums.	`disable`
`is-type {level-1 | level-1-2 | level-2-only}`	Set the ISIS level to use. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both).	`level-1-2`
`lsp-gen-interval-l1 <interval_int>`	Minimum interval for level 1 link state packet (LSP) regenerating. Range 1 to 120.	`30`
`lsp-gen-interval-l2 <interval_int>`	Minimum interval for level 2 LSP regenerating. Range 1 to 120.	`30`
`lsp-refresh-interval <interval_int>`	LSP refresh time in seconds. Range 1 to 65535 seconds.	`900`
`max-lsp-lifetime <lifetime_int>`	Maximum LSP lifetime in seconds. Range 350 to 65535 seconds.	`1200`
`metric-style {narrow | narrow-transition | narrow-transition-l1 | narrow-transition-l2 | transition | transition-l1 | transition-l2 | wide | wide-l1 | wide-l2 | wide-transition | wide-transition-l1 | wide-transition-l2}`	Use old-style (ISO 10589) or new-style packet formats. • `narrow` Use old style of TLVs with narrow metric. • `narrow-transition narrow`, and accept both styles of TLVs during transition. • `narrow-transition-l1` narrow-transition level-1 only. • `narrow-transition-l2` narrow-transition level-2 only. • `transition` Send and accept both styles of TLVs during transition. • `transition-l1` transition level-1 only. • `transition-l2` transition level-2 only. • `wide` Use new style of TLVs to carry wider metric. • `wide-l1` wide level-1 only. • `wide-l2` wide level-2 only. • `wide-transition` wide, and accept both styles of TLVs during transition. • `wide-transition-l1` wide-transition level-1 only. • `wide-transition-l2` wide-transition level-2 only.	`narrow`
`overload-bit {disable | enable}`	Signal other routers not to use us in SPF.	`disable`
`overload-bit-on-startup`	Set overload-bit only temporarily after reboot. Range is 5-86400 seconds. Enter `unset overload-bit-on-startup` to disable. Entering `set overload-bit-on-startup 0` is invalid.	`0`
`overload-bit-suppress external interlevel`	Suppress overload-bit for the specific prefixes. You can suppress the overload-bit for external prefixes, internal prefixes or both. Enter `unset overload-bit-suppress` to disable.	
`redistribute-l1 {disable | enable}`	Redistribute level 1 routes into level 2. If enabled, configure `redistribute-l1-list`.	`disable`
`redistribute-l1-list <access_list_str>`	Access-list for redistribute l1 to l2. Available if `redistribute-l1` enabled.	`(null)`
`redistribute-l2 {disable | enable}`	Redistribute level 2 routes into level 1. If enabled, configure `redistribute-l2-list`.	`disable`

Variable	Description	Default
redistribute-l2-list <access_list_str>	Access-list for redistribute l2 to l1. Available if redistribute-l2 enabled.	(null)
spf-interval-exp-l1 <minimum_delay_int> <l	Level 1 SPF calculation delay in milliseconds. Enter the maximum and maximum delay between receiving a change to the level 1 SPF calculation in milliseconds.	500 50000
spf-interval-exp-l2 <min_delay_int> <max_delay_int>	Level 2 SPF calculation delay. Enter the maximum and maximum delay between receiving a change to the level 2 SPF calculation in milliseconds.	500 50000

config isis-interface

Configure and enable FortiGate unit interfaces for IS-IS.

Variable	Description	Default
edit <interface_str>	Edit an IS-IS interface.	
auth-keychain-l1 <keychain_str>	Authentication key-chain for level 1 PDUs. Available when auth-mode-l1 is set to md5.	
auth-keychain-l2 <keychain_str>	Authentication key-chain for level 2 PDUs. Available when auth-mode-l2 is set to md5.	
auth-mode-l1 {md5 | password}	Level 1 authentication mode.	password
auth-mode-l2 {md5 | password}	Level 2 authentication mode.	password
auth-password-l1 <password>	Authentication password for level 1 PDUs. Available when auth-keychain-11 is set to password.	
auth-password-l2 <password>	Authentication password for level 2 PDUs. Available when auth-keychain-12 is set to password.	
auth-send-only-l1 {disable | enable}	Level 1 authentication send-only.	disable
auth-send-only-l2 {disable | enable}	Level 2 authentication send-only.	disable
circuit-type {level-1 | level-1-2 | level-2-only}	Set the ISIS circuit type to use for the interface. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both).	level-1-2
csnp-interval-l1 <interval_int>	Level 1 CSNP interval. The range is 1-65535 seconds.	10
csnp-interval-l2 <interval_int>	Level 2 CSNP interval. The range is 1-65535 seconds.	10
hello-interval-l1 <interval_int>	Level 1 hello interval. The range is 1-65535 seconds. Set to 0 for a one-second hold time.	10
hello-interval-l2 <interval_int>	Level 2 hello interval. The range is 1-65535 seconds. Set to 0 for a one-second hold time.	10
hello-multiplier-l1 <multipler_int>	Level 1 multiplier for Hello holding time. The range is 2 to 100.	3
hello-multiplier-l2 <multipler_int>	Level 2 multiplier for Hello holding time. The range is 2 to 100.	3
hello-padding {disable | enable}	Enable or disable adding padding to IS-IS hello packets.	disable

Variable	Description	Default
`lsp-interval <interval_int>`	LSP transmission interval (milliseconds). The range is 1-4294967295.	`33`
`lsp-retransmit-interval <interval_int>`	LSP retransmission interval (seconds). The range is 1-65535.	`5`
`mesh-group {disable | enable}`	Enable IS-IS mesh group.	`disable`
`mesh-group-id <id_int>`	Mesh group ID. The range is 0-4294967295. A value of 0 means the mesh group is blocked.	`0`
`metric-l1 <metric_int>`	Level 1 metric for interface. The range is 1-63.	`10`
`metric-l2 <metric_int>`	Level 2 metric for interface. The range is 1-63.	`10`
`network-type {broadcast | point-to-point}`	Set the IS-IS interface's network type.	
`priority-l1 <priority_int>`	Level 1 priority. The range is 0-127.	`64`
`priority-l2 <priority_int>`	Level 2 priority. The range is 0-127.	`64`
`status {disable | enable}`	Enable the interface for IS-IS.	`disable`
`wide-metric-l1 <metric_int>`	Level 1 wide metric for the interface. The range is 1-16777214.	`10`
`wide-metric-l2 <metric_int>`	Level 2 wide metric for the interface. The range is 1-16777214.	`10`

config isis-net

Add IS-IS networks.

Variable	Description	Default
`edit <id>`	Add the ID number of the IS-IS network	
`net <user_defined>`	Enter a user defined IS-IS network in the form xx.xxxx. ... .xxxx.xx.	:

config redistribute {bgp | connected | ospf | rip | static}

Redistribute routes from other routing protocols using IS-IS.

Variable	Description	Default
`status {disable | enable}`	Enable or disable redistributing the selected protocol’s routes.	`disable`
`protocol {bgp | connected | ospf | rip | static}`	The name of the protocol that to redistribute ISIS routes to.	
`metric <metric_int>`	Set the metric. Range is 0-4261412864.	`0`

Variable	Description	Default
`metric-type {external	internal}`	Set the metric type.	`internal`
`level {level-1	level-1-2	level-2}`	Set the ISIS level type to use for distributing routes. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both).	`level-2`
`routemap <routmap_name>`	Enter a routemap name.	`(null)`

config summary-address

Add IS-IS summary addresses.

Variable	Description	Default
`edit <id>`	Add the ID number of the summary address.	
`level {level-1	level-1-2	level-2}`	Set the ISIS level to use for the summary database. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both).	`level-2`
`prefix <prefix_ipv4> <prefix_mask>`	The summary address prefix and netmask.	`0.0.0.0 0.0.0.0`

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.

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 212.	`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 212. 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 212.	`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 212.	`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 212.	`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 212. 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 212. 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 212. 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 212. 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.`

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 453.	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 212.	`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 257.

You can use access or prefix lists for OSPF area filter lists. For more information, see “access-list, access-list6” on page 212 and “prefix-list, prefix-list6” on page 273.

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 257.

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 257). 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 261.	`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 255.	`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 212.

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 260.	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.
- `isis` — Redistribute routes learned from ISIS.
- `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 | isis | 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 288.	`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 257. 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`

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 253.

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 257.

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 257). 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.
- isis — Redistribute routes learned from ISIS.
- 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 | isis | 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`

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 2: 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 6 (TCP), 17 (UDP), and 132 (SCTP) 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 (TCP), 17 (UDP), and 132 (SCTP) 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 6 (TCP), 17 (UDP), and 132 (SCTP) 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.

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 294.

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`

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 280 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 279.	`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 212.	`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 212 and "prefix-list, prefix-list6" on page 273.

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 240.	`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 276 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 212.	`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.
- `isis` — Redistribute routes learned from ISIS.
- `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 | isis | 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 288.	`Null.`
`status {enable | disable}`	Enable or disable advertising non-RIP routes.	`disable`

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 280 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 212 and “router prefix-list, prefix-list6” on page 273.

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 276 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.
- `isis` — Redistribute routes learned from ISIS.
- `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 | isis | 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`

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 290, and RIP "config redistribute" on page 263.

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 290.

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 220), 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		

Variable	Description	Default
`edit <route_map_rule_id>`	Enter an entry number for the rule. The number must be an integer.	No 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 214.	`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 232.	`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 221).	`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 223).	`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 232).	`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 220.	`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 220.	`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 220.	`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`

setting

Use this command to define a prefix list as a filter to show routes.

Command

```
config router setting
  set hostname <name_str>
  set show-filter <prefix_list>
end
```

Variable	Description	Default
`hostname <name_str>`	Enter the hostname for this virtual domain router. 1-14 characters.	
`show-filter <prefix_list>`	Select the prefix-list to use as a filter for showing routes.	

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 297.

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. ECMP is available to static and OSPF routing. By default in ECMP, a source IP address hash will be used to determine the selected route. This hash value is based on the pre-NATed source IP address. This method results in all traffic originating from the same source IP address always using the same path. This is the Source based ECMP option, with Weighted, and Spill-over being the other two optional methods. The option is determined by the CLI command `set v4-ecmp-mode` in `config system setting`. Source Based is the default method. Weighted ECMP uses the weight field to direct more traffic to routes with larger weights. In spill-over or usage-based ECMP, the FortiGate unit distributes sessions among ECMP routes based on how busy the FortiGate interfaces added to the routes are. For more information on ECMP, see “system settings” on page 452.

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`

Variable	**Description**	**Default**
`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`
`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 IP source hash (based on the pre-NATed IP address) for the routes will be used to determine which route is selected.The priority 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 452.	0

static6

Use this command to add, edit, or delete static routes for IPv6 traffic. For IPv4 static routes, see “static” on page 295.

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 distance <distance>
    set dst <destination-address_ipv6mask>
    set gateway <gateway-address_ipv6>
    set priority <integer>
  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.`
`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`
`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.	`::`
`priority <integer>`	The administrative priority value is used to resolve ties in route selection. The priority range is an integer from 0 to 4294967295. Lower priority routes are preferred routes. This field is only accessible through the CLI.	0

•

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.

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, 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.	`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, the message is processed according to the spam action setting. 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`

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 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 349.

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`

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 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

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 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 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.

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

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 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.	`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`

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

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 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.	`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`

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

profile

Use this command to configure UTM email filtering profiles for firewall policies. Email filtering profiles configure how Email filtering and FortiGuard Antispam is applied to sessions accepted by a firewall policy that includes the Email filtering profile.

Syntax

```
config spamfilter profile
  edit <name_str>
    set comment <comment_str>
    set spam-log {disable | enable}
    set spam-bword-threshold <value_int>
    set spam-bword-table <index_int>
    set spam-emaddr-table <index_int>
    set spam-ipbwl-table <index_int>
    set spam-mheader-table <index_int>
    set spam-rbl-table <index_int>
    set spam-iptrust-table <index_int>
      config config {imap | imaps | pop3 | pop3s | smtp | smtps}
        set options {bannedword | spamemailbwl | spamfschksum | spamfsip |
            spamfssubmit | spamfsurl | spamhdrcheck | spamipbwl |
            spamraddrdns | spamrbl}
        set action {discard | pass | tag}
        set tag-type {subject | header} [spaminfo]
        set tag-msg <message_str>
        set hdrip {disable | enable}
        set local-override {enable | disable}
    end
end
```

Variable	Description	Default
`<name_str>`	Enter the name of the email filtering profile.	
`comment <comment_str>`	Optionally enter a description of up to 63 characters of the email filter profile.	
`spam-log {disable | enable}`	Enable or disable logging for email filtering.	`disable`
`spam-bword-threshold <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
`spam-bword-table <index_int>`	Enter the ID number of the email filter banned word list to be used.	`0`
`spam-emaddr-table <index_int>`	Enter the ID number of the email filter email address list to be used.	`0`
`spam-ipbwl-table <index_int>`	Enter the ID number of the email filter IP address black/white list to be used with the profile.	`0`
`spam-mheader-table <index_int>`	Enter the ID number of the email filter MIME header list to be used with the profile.	`0`
`spam-rbl-table <index_int>`	Enter the ID number of the email filter DNSBL list to be used with the profile.	`0`
`spam-iptrust-table <index_int>`	Enter the ID number of the email filter IP trust list to be used with the profile.	`0`

config {imap | imaps | pop3 | pop3s | smtp | smtps}

Configure spam filtering options for the IMAP, IMAPS, POP3, POP3S, SMTP, and SMTPS email protocols.

Variable	Description	Default
`options {bannedword | spamemailbwl | spamfschksum | spamfsip | spamfssubmit | spamfsurl | spamhdrcheck | spamipbwl | spamraddrdns | spamrbl}`	Select actions, if any, the FortiGate unit will perform with SMTP connections. • `bannedword` block email containing content in the banned word list. • `spamemailbwl` filter email using the email filtering black/white list. • `spamfsip` filter email using the FortiGuard Antispam filtering IP address blacklist. • `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` filter email using the FortiGuard Antispam filtering URL blacklist. • `spamhdrcheck` filter email using the MIME header list. • `spamipbwl` filter email using a return email DNS check. • `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. 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`
`action {discard | pass | tag}`	Select the action that this profile uses for filtered 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 spam. `discard` do not pass email identified as spam. `pass` disable spam filtering. `tag` tag spam email with text configured using the `tagmsg` option and the location set using the `tag-type` option.	`discard`
`tag-type {subject | header} [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 `tag-msg`. If you select to add 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.	`subject` `spaminfo`
`tag-msg <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. Tagging text using other encodings may not be accepted. 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`
`hdrip {disable | enable}`	For `smtp` and `smtps`. Select to check header IP addresses for `spamfsip, spamrbl,` and `spamipbwl` filters.	`disable`

Variable	**Description**	**Default**
`local-override {enable | disable}`	For `smtp` and `smtps`. Select to override SMTP or SMTPS remote check, which includes IP RBL check, IP FortiGuard antispam check, and HELO DNS check, with the locally defined black/white antispam list.	`disable`

system

Use `system` commands to configure options related to the overall operation of the FortiGate unit, including. This chapter contains the following sections:

accprofile
admin
alertemail
amc
amc-slot
arp-table
auto-install
autoupdate clientoverride
autoupdate override
autoupdate push-update
autoupdate schedule
autoupdate tunneling
aux
bug-report
central-management
carrier-endpoint-translation
chassis-loadbalance
console
dhcp reserved-address
dhcp server
dns
dns-database
dynamic-profile
fips-cc
fortiguard
fortiguard-log
gi-gk
global
gre-tunnel
ha
interface
ipv6-tunnel
mac-address-table
modem
npu
ntp
password-policy
proxy-arp
replacemsg admin
replacemsg alertmail
replacemsg auth
replacemsg ec
replacemsg fortiguard-wf
replacemsg ftp
replacemsg http
replacemsg im
replacemsg mail
replacemsg mm1
replacemsg mm3
replacemsg mm4
replacemsg mm7
replacemsg-group
replacemsg-group
replacemsg-image
replacemsg nac-quar
replacemsg nntp
replacemsg spam
replacemsg sslvpn
replacemsg traffic-quota
resource-limits
session-helper
session-sync
session-ttl
settings
sit-tunnel
sflow
snmp community
snmp sysinfo
snmp user
storage
switch-interface
tos-based-priority
vdom-dns
vdom-link
vdom-property
vdom-sflow
wccp
wireless ap-status
wireless settings
zone

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. For future use.	`none`

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 web-based manager 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.

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 storage
          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
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

Variable	Description	Default
`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`
`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.

Variable	Description	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 `storage` — Storage 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, 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.	
`storage`	Set the dashboard column and open and closed status of the log and archive storage 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.	

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 29.

Syntax

```
config system alertemail
  set authenticate {disable | enable}
  set password <password_str>
  set port <port_integer>
  set server {<name-str> | <address_ipv4>}
  set source-ip <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.
`source-ip <address_ipv4>`	Enter the SMTP server source IP address.	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.

amc

Use this command to configure AMC ports on your FortiGate unit.

Syntax

```
config system amc
  set {dw1 | dw2} {adm-fb8 | adm-fe8 | adm-xb2 | adm-xd4 | adm-xe2 | auto |
      none}
  set {sw1 | sw2} {asm-ce4 | asm-cx4 | asm-disk | asm-fb4 | asm-et4 | asm-fx2
      | auto | none}
end
```

Variable	Description	Default
`{dw1	dw2} {adm-fb8	adm-fe8	adm-xb2	adm-xd4	adm-xe2	auto	none}`	Configure this double width AMC slot for the following type of module. `adm-fb8` AMC double width 8G NP2 accelerated network interface module `adm-fe8` AMC double width 8G FE8 accelerated network interface module `adm-xb2` AMC double width 2XG NP2 accelerated network interface module `adm-xd4` AMC double width 4XG XD4 accelerated network interface module `adm-xe2` AMC double width 2XG XE2 accelerated network interface module `auto` support any card that is inserted none not configured, disable slot	`auto`
`{sw1	sw2} {asm-ce4	asm-cx4	asm-disk	asm-fb4	asm-et4	asm-fx2	auto	none}`	Configure this single width AMC port for the following type of card. `asm-ce4` AMC single width, 4G CE4 accelerated network interface module `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 accelerated network interface module `asm-et4` AMC single width T1/E1 network interface module `asm-fx2` AMC single width, 2G bypass `auto` support any single width card none not configured, disable slot	`auto`

amc-slot

Use this command to configure settings for the modules installed in AMC slots. The settings that you can configure depend on the card actually installed in the slot.

Syntax

```
config system amc-slot
  edit {dw1 | dw2 | sw1 | sw2}
    set optimization-mode {fw-ips | fw-only-hash | fw-only-round-robin}
    set ips-weight {all-ips | balanced | less-fw}
    set ips-p2p( disable | enable}
    set ips-fail-open (disable | enable}
    set fp-disable {Dos | all | ips | ipsec | multicast | none}
    set ipsec-inb-optimization (disable | enable}
    set syn-proxy-client-timer <timer_int>
    set syn-proxy-server-timer <timer_int>
end
```

Variable	Description	Default
`edit {dw1 | dw2 | sw1 | sw2}`	Edit and AMC slot to change the configuration of the module installed in the slot.	
`optimization-mode {fw-ips | fw-only-hash | fw-only-round-robin}`	Set performance optimization mode for module in the AMC slot. `fw-ips` optimize for both firewall and IPS acceleration. `fw-oly-hash` optimize for firewall acceleration using hash mode. `fw-oly-hash` optimize for firewall acceleration using round-robin mode.	`fw-ips`
`ips-weight {all-ips | balanced | less-fw}`	Set the IPS weight. `all-ips` all AMC module processing resources are used for IPS `balanced` balance AMC module processing resources for firewall and IPS. `less-fw` reduced AMC module processing resources for firewall sessions.	`balanced`
`ips-p2p( disable | enable}`	Enable or disable IPS P2P acceleration.	`disable`
`ips-fail-open (disable | enable}`	Enable or disable IPS failopen. If enabled, if the IPS engine crashes traffic flow is maintained but is not checked by IPS. If disabled, traffic is blocked if the IPS engine crashes.	`enable`
`fp-disable {Dos | all | ips | ipsec | multicast | none}`	Disable fast path processing for none, one, or multiple features. DoS disable fast path processing for DoS protection. `all` disable all fast path processing. `ips` disable fast path processing for IPS sensors. `ipsec` disable fast path processing for IPsec VPN. `multicast` disable fast path processing for multicast forwarding. `none` enable all fast path processing.	`none`
`ipsec-inb-optimization (disable | enable}`	Enable or disable acceleration of IPsec inbound traffic.	`enable`
`syn-proxy-client-timer <timer_int>`	The syn proxy's client timer interval in seconds. Range is 1 to 255.	3
`syn-proxy-server-timer <timer_int>`	The syn proxy's server timer interval in seconds. Range is 1 to 255.	3

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.

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`

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.

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 364.

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`

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

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`

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.

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 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.

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.

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 status {enable | disable}
  set type { fortiguard | fortimanager }
  set auto-backup {enable | disable}
  set copy-local-revision {enable | disable}
  set schedule-config-restore {enable | disable}
  set schedule-script-restore {enable | disable}
  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 serial-number <fmg_serial_number>
  set fmg <fmg_ipv4>
  set fmg-source-ip <address_ipv4>
  set vdom <name_string>
end
```

Variable	Description	Default
`status {enable | disable}`	Select to enable remote management service for your FortiGate unit.	`disable`
`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`
`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`
`copy-local-revision {enable | disable}`	Enable sending a copy to the management station when storing the configuration to a flash disk.	`disable`
`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`
`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`

Variable	Description	Default
`allow-monitor {enable | disable}`	Select to allow the remote service to monitor your FortiGate unit.	`disable`
`authorized-manager-only {enable | disable}`	Select to restrict access to the authorized manger only.	`disable`
`serial-number <fmg_serial_number>`	Enter the serial number of the remote FortiManager server.	`null`
`fmg <fmg_ipv4>`	Enter the IP address or FQDN of the remote FortiManager server.	`null`
`fmg-source-ip <address_ipv4>`	Enter the source IP address to use when connecting to FortiManager.	`null`
`vdom <name_string>`	Enter the name of the vdom to use when communicating with the FortiManager unit. This field is optional.	`root`

carrier-endpoint-translation

Use this command to configure FortiOS Carrier carrier end point HTTP header options. HTTP header options control how FortiOS Carrier finds source IP addresses and carrier end points in communication sessions. In most cases you do not have to change the default settings. The default settings assumes that the source IP address of communication sessions is the actual IP address of the originator of the communication session. The default settings also causes FortiOS Carrier to look in the HTTP header for the carrier end point.

However, some types of traffic are exceptions that require selecting one of the other Profile Query types and adding additional configuration settings. An important exception is WAP traffic because, which comes from a WAP server instead of directly from a customer so extra configuration is required for WAP traffic.

Syntax

```
config system carrier-endpoint-translation
  set carrier-endpoint-convert-hex {enable | disable}
  set carrier-endpoint-header <endpoint_header_title>
  set carrier-endpoint-header-suppress {enable | disable}
  set carrier-endpoint-prefix {enable | disable}
  set carrier-endpoint-prefix-range-max <prefix_range_max>
  set carrier-endpoint-prefix-range-min <prefix_range_min>
  set carrier-endpoint-prefix-string <prefix_string>
  set carrier-endpoint-source {cookie | http-header}
  set profile-query-type {extract-carrier-endpoint | extract-ip | session-
     ip}
  set ip-header <ip_header_name>
  set ip-header-suppress {enable | disable}
  set missing-header-fallback <policy-profile | session-ip>
end
```

Variable	Description	Default
`carrier-endpoint-convert-hex {enable	disable}`	Enable if the carrier end point is encoded in the communication session using hexadecimal notation. FortiOS Carrier converts the carrier end point from hex to decimal.	disable
`carrier-endpoint-header <endpoint_header_title>`	Specify the header field in the communication session that includes the carrier end point.	x-up-calling-line-id
`carrier-endpoint-header-suppress {enable	disable}`	Enable to delete the carrier end point header found in the specified `carrier-endpoint-header` field. You can use this feature to prevent your customer’s carrier end points from appearing on the Internet.	`disable`
`carrier-endpoint-prefix {enable	disable}`	Enable to add a prefix to the carrier end point found in the communication session. The other `carrier-endpoint-prefix` fields are available only of `carrier-endpoint-prefix` is enabled.	`disable`
`carrier-endpoint-prefix-range-max <prefix_range_max>`	Maximum number of characters in the carrier endpoint prefix string. Range is integer 1 - 16. The carrier endpoint prefix is not added to the carrier end point if the carrier end point has the same or more digits than the maximum number of characters. Only available if `carrier-endpoint-prefix` is enabled.	`null`
`carrier-endpoint-prefix-range-min <prefix_range_min>`	Minimum number of characters in the carrier endpoint prefix string. Range is integer 1 - 16. The prefix is not added to the carrier end point if it has the same or fewer digits than the minimum length. Only available if `carrier-endpoint-prefix` is enabled.	`null`

Variable	Description	Default
`carrier-endpoint-prefix-string <prefix_string>`	The alphanumeric string that is the prefix to add to the carrier end point. Only available if `carrier-endpoint-prefix` is enabled.	`null`
`carrier-endpoint-source {cookie | http-header}`	Configure FortiOS Carrier to find the communication session's carrier end point in the HTTP Header Field (`http-header`) or in a Cookie (`cookie`) in the HTTP session.	http-header
`profile-query-type {extract-carrier-endpoint | extract-ip | session-ip}`	Select the specific type of dynamic profile query to be executed: **session-ip** — Default setting. Use the actual source IP address of the communication session and the carrier end point extracted from the communication session. **extract-ip** — Use the actual source IP address of communication sessions and get the carrier end point from the user context list. Configure HTTP header options to get the IP address from communication sessions. **extract-endpoint** — Extract the carrier end point from communication sessions and get the source IP address from the user context list. Configure HTTP header options to get the carrier end point from communication sessions.	session-ip
`ip-header <ip_header_name>`	Specify the header field in the communication session that includes the source IP address. Only available if `profile-query-type is session-ip`. Up to 64 character maximum.	X-Up-Forwarded-For
`ip-header-suppress {enable | disable}`	Enable to delete the IP address header found in the IP address header field specified by the `ip-header` field. You can use this feature to prevent your customers source IP addresses from appearing on the Internet. Only available if `profile-query-type is session-ip.`	disable
`missing-header-fallback <policy-profile | session-ip>`	Specify how to get the source IP address of the communication session. FortiOS Carrier matches this IP address with the IP addresses in the user context list. Select **policy-profile** — use the IP address found in the specified `ip-header`. **session-ip** — use the actual source IP address of the communication session. Use this option if FortiOS Carrier cannot find the specified IP address header or if the specified IP address header does not contain an IP address.	policy-profile

chassis-loadbalance

Use this command to set the console command mode, the number of lines displayed by the console, and the baud rate.

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 chassis-loadbalance
  set data-port
  set status {disable | enable}
  set switch-port
  config conf-sync
    set status {enable | disable}
    set domain-id <int>
    set heartbeat-interval <int>
    set heartbeat-lost-threshold <packets_int>
    set mgmt-gateway <ipv4_ip>
    set password <str>
  end
end
```

Variable	Description	Default
`data-port`	Set the console port baudrate. Select one of 9600, 19200, 38400, 57600, or 115200.	`9600`
`status {disable | enable}`	Set the console mode to line or batch. Used for autotesting only.	`line`
`switch-port`	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
`config conf-sync` **fields**		
`status {enable | disable}`	Enable/disable configuration sync.	`disable`
`domain-id <int>`	Enter the domain ID. Range 0-255.	0
`heartbeat-interval <int>`	Heartbeat interval 1-20 x 100ms.	2
`heartbeat-lost-threshold <packets_int>`	Heartbeat lost threshold. Range 1-60 lost packets.	6
`mgmt-gateway <ipv4_ip>`	Gateway ip for management interface.	0.0.0.0
`password <str>`	Password.	

console

Use this command to set the console command mode, the number of lines displayed by the console, and the baud rate.

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

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 346.

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`

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 345.

This command is available in NAT/Route mode only.

Syntax

```
config system dhcp server
  edit <server_index_int>
    set conflicted-ip-timeout <timeout_int>
    set default-gateway <address_ipv4>
    set dns-service {default | specify}
    set domain <domain_name_str>
    set enable {enable | disable}
    set interface <interface_name>
    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 {ipsec | regular}
    set start-ip <address_ipv4>
    set wins-server1 <wins_ipv4>
    set wins-server2 <wins_ipv4>
    set wins-server3 <wins_ipv4>
    set dns-server1 <address_ipv4>
    set dns-server2 <address_ipv4>
    set dns-server3 <address_ipv4>
    set ip-mode {range | usrgrp}
    set ipsec-lease-hold <release_seconds>
    config exclude-range
      edit <excl_range_int>
        set end-ip <end_ipv4>
        set start-ip <start_ipv4>
    config ip-range
      edit <ip_range_int>
        set end-ip <end_ipv4>
        set start-ip <start_ipv4>
    end
  end
```

Variable	Description	Default
`edit <server_index_int>`	Enter an integer ID for the DHCP server. The sequence number may influence routing priority in the FortiGate unit forwarding table.	
`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`

Variable	Description	Default
`dns-service {default | specify}`	Select `default` to assign DHCP clients the DNS servers added to the FortiGate unit using the `config system dns` command. Select `specify` to specify the DNS servers that this DHCP server assigns to DHCP clients. Use the `dns-server#` options to add DNS servers to this DHCP server configuration.	`specify`
`domain <domain_name_str>`	Domain name suffix for the IP addresses that the DHCP server assigns to DHCP clients.	
`enable {enable | disable}`	Enable or disable this DHCP server.	`enable`
`interface <interface_name>`	The FortiGate unit interface that this DHCP server can assign IP addresses from. Devices connected to this interface can get their IP addresses from this DHCP server. You can only add one DHCP server to an interface.	
`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.	`604800 (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.	`0`

`server-type {ipsec | regular}`	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`
`wins-server3 <wins_ipv4>`	The IP address of the third WINS server 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. Used if `dns-service` is set to `specify`.	`0.0.0.0`
`dns-server2 <address_ipv4>`	The IP address of the second DNS server that the DHCP server assigns to DHCP clients. Used if `dns-service` is set to `specify`.	`0.0.0.0`
`dns-server3 <address_ipv4>`	The IP address of the third DNS server that the DHCP server assigns to DHCP clients. Used if `dns-service` is set to `specify`.	`0.0.0.0`
`ip-mode {range | usrgrp}`	Configure whether an IPsec DHCP server assigns IP addresses based on the IP address range added to the configuration or based on the user group of the IPsec VPN user. Visible only when `server-type` is set to `ipsec`.	`range`
`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`

Variable	Description	Default
`config exclude-range`	Configure a range of IP addresses to exclude from the list of DHCP addresses that are available.	
`config ip-range`	Configure the range of IP addresses that this DHCP server can assign to DHCP clients.	
`edit <excl_range_int>`	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.	
`edit <ip_range_int>`	Enter an integer ID for this IP address range. You can add up to 16 ranges of IP addresses that the FortiGate DHCP server can assign to DHCP clients.	
`start-ip <start_ipv4>`	The start IP address in the exclusion range. The start IP and end IP must be in the same subnet.	`0.0.0.0`
`end-ip <end_ipv4>`	The end IP address in the exclusion range. The start IP and end IP must be in the same subnet.	`0.0.0.0`

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

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`

dynamic-profile

MSSP and carrier service providers can use the FortiOS Carrier dynamic profile configuration to dynamically assign profile groups to customer traffic. Using the dynamic profile, FortiOS Carrier can receive RADIUS Start records from service provider accounting systems when customers connect to service provider networks. In real time FortiOS Carrier can extract identifying information and profile group names from these RADIUS Start records and match the identifying information with the customer communication session. FortiOS Carrier can then dynamically select and apply the profile group named in the RADIUS Start record to the communication session.

Syntax

```
config system dynamic-profile
  set context-timeout <timeout_seconds>
  set carrier-endpoint-attribute <RADIUS_attribute>
  set hold-time <proxy_hold_time>
  set log-flags <lflags>
  set log-period <log_time>
  set mem-percent <memory_percent>
  set profile-attribute <RADIUS_attribute>
  set profile-attribute-key <profile_attribute_key>
  set radius-response {enable | disable}
  set radius-server-port <RADIUS_listen_port>
  set secret <server_password>
  set status
  set status-ftgd
  set status-ftp
  set status-http
  set status-imap
  set status-im-ips
  set status-log
  set status-nntp
  set status-pop3
  set status-smtp
  set validate-request-secret {enable | disable}
  set vdom <vdom-name>
end
```

Variable	Description	Default
`context-timeout <timeout_seconds>`	The number of seconds that a user context entry can remain in the user context list without FortiOS Carrier receiving a communication session from the carrier end point. If a user context entry is not being looked up, then the user must no longer be connected to the network. This timeout is only required if FortiOS Carrier doesn't receive the RADIUS Stop record. However, even if the accounting system does send RADIUS Stop records this timeout should be set in case FortiOS Carrier misses a Stop record. The default user context entry timeout is 28800 seconds (8 hours). You can keep this timeout relatively high because its not usually a problem to have a long list, but entries that are no longer used should be removed regularly. You might want to reduce this timeout if the accounting server does not send RADIUS Stop records. Also if customer IP addresses change often you might want to set this timeout lower so that out of date entries are removed from the list. If this timeout is too low FortiOS Carrier could remove user context entries for users who are still connected. Set the timeout to 0 if you do not want FortiOS Carrier to remove entries from the list except in response to RADIUS Stop messages.	28800
`carrier-endpoint-attribute <RADIUS_attribute>`	To extract the carrier end point from the RADIUS Start record, this field must be set to the name of the RADIUS attribute that contains the carrier end point. You can select the `RADIUS_attribute` from the list or enter an attribute name. The `RADIUS_attribute` must match one of the RADIUS attributes in the list. The `RADIUS_attribute` is case sensitive.	Calling-Station-Id
`hold-time <proxy_hold_time>`	If FortiOS Carrier receives a communication session and can't find a corresponding carrier end point and IP address in the user context list, the system waits for the user context creation timeout. If a match is not found after this timeout, FortiOS Carrier applies the profile group in the firewall policy to the communication session. The default user context creation timeout is 5 seconds. You might want to increase this timeout if the default profile group is being applied to users instead of the profile group that should be dynamically assigned. This could be happening if there is a delay before FortiOS Carrier receives the RADIUS Start record from the accounting server. If you set this timeout to `0` FortiOS Carrier blocks communication sessions that do not have a matching entry in the user context list.	5

Variable	Description	Default
`log-flags <lflags>`	Enter one or more of the following options to configure FortiOS Carrier to write event log messages for dynamic profile events. You can enter multiple options. Separate the options with a space. none Disable writing event log messages for dynamic profile events. accounting-event Enable to write an event log message when FortiOS Carrier does not find the expected information in a RADIUS Record. For example, if a RADIUS record contains more than the expected number of addresses. accounting-stop-missed Enable to write an event log message whenever a user context entry timeout expires indicating that FortiOS Carrier removed an entry from the user context list without receiving a RADIUS Stop message. context-missing Enable to write an event log message whenever a user context creation timeout expires indicating that FortiOS Carrier was not able to match a communication session because a matching entry was not found in the user context list. profile-missing Enable to write an event log message whenever FortiOS Carrier cannot find a profile group name in a RADIUS start message that matches the name of a profile group added to FortiOS Carrier. protocol-error Enable to write an event log message if RADIUS protocol errors occur. For example, if a RADIUS record contains a RADIUS secret that does not match the one added to the dynamic profile. radiusd-other Enable to write event log messages for other events. The event is described in the log message. For example, write a log message if the memory limit for the user context list is reached and the oldest entries in the table have been dropped.	All options except `none`.
`log-period <log_time>`	The time in seconds to group event log messages for dynamic profile events. For example, if the log message period is 30 seconds, FortiOS Carrier generates groups of event log messages every 30 seconds instead of generating event log messages continuously. And the log messages generated each period contain a count of how many events of that type occurred. If set to 0, FortiOS Carrier generates all event log messages in real time.	0
`mem-percent <memory_percent>`	Maximum percentage of system memory to use for the user context tables. CLI only. The range is 1 to 25%.	4
`profile-attribute <RADIUS_attribute>`	To extract a profile group name from the RADIUS Start record, this field must be set to the name of the RADIUS attribute that contains the profile group name. You can select the `RADIUS_attribute` from the list or enter an attribute name. The `RADIUS_attribute` must match one of the RADIUS attributes in the list. The `RADIUS_attribute` is case sensitive.	`Class`

Variable	Description	Default
`profile-attribute-key <profile_attribute_key>`	Enter a string if the profile attribute contains more data than just the profile group name. The profile key is a text string that always comes directly before the profile group name in the profile attribute. For example, if the profile group name always follows the text string `profile`, the class attribute could include the string: `profile=<profile_name_str>`. Where `<profile_name_str>` is the name of the profile group. Maximum 36 characters.	`No default.`
`radius-response {enable | disable}`	Enable if you want FortiOS Carrier to send RADIUS responses after receiving RADIUS Start and Stop records. This setting may be required by your accounting system.	`disable`
`radius-server-port <RADIUS_listen_port>`	If required, change the UDP port number used by the RADIUS accounting server for sending RADIUS records. FortiOS Carrier listens for RADIUS Start and Stop records on this port.	1813
`secret <server_password>`	Enter the RADIUS secret used by the RADIUS accounting server.	`No default.`
`status`	Enable the dynamic profile and then configure dynamic profile settings. When you enable the dynamic profile, FortiOS Carrier accepts connections on the `radius-server-port`. As well, FortiOS Carrier attempts to dynamically assign a profile group to all communication sessions accepted by any firewall policy that includes a profile group. Dynamically assigning a profile group occurs only if a match is found between the carrier end point and source IP address in the communication session and a carrier end point and source IP address received in a RADIUS Start record and then only if the RADIUS Start record includes a profile group name.	`disable`
`status-ftgd`	Enable to dynamically assign profile groups to sessions that include FortiGuard overrides. Disable to exempt sessions that include FortiGuard overrides from being dynamically assigned profile groups.	`enable`
`status-ftp`	Enable to dynamically assign profile groups to FTP sessions that are accepted by firewall policies that contain a profile group. Disable to exempt FTP sessions from being dynamically assigned profile groups.	`enable`
`status-http`	Enable to dynamically assign profile groups to HTTP, MM1, and MM7 sessions that are accepted by firewall policies that contain a profile group. Disable to exempt HTTP, MM1, and MM7 sessions from being dynamically assigned profile groups.	`enable`
`status-imap`	Enable to dynamically assign profile groups to IMAP sessions that are accepted by firewall policies that contain a profile group. Disable to exempt IMAP sessions from being dynamically assigned profile groups.	`enable`
`status-im-ips`	Enable to dynamically assign profile groups to IM, IPS, and VOIP sessions that are accepted by firewall policies that contain a profile group. Disable to exempt IM, IPS, and VOIP sessions from being dynamically assigned profile groups.	`enable`
`status-log`	Enable to insert the appropriate carrier end point into all log messages generated by FortiOS Carrier when these log messages are generated by events related to processing a carrier end point communication session.	`enable`
`status-nntp`	Enable to dynamically assign profile groups to NNTP sessions that are accepted by firewall policies that contain a profile group. Disable to exempt NNTP sessions from being dynamically assigned profile groups.	`enable`
`status-pop3`	Enable to dynamically assign profile groups to POP3 sessions that are accepted by firewall policies that contain a profile group. Disable to exempt POP3 sessions from being dynamically assigned profile groups.	`enable`

Variable	Description	Default
`status-smtp`	Enable to dynamically assign profile groups to SMTP sessions that are accepted by firewall policies that contain a profile group. Disable to exempt SMTP sessions from being dynamically assigned profile groups.	`enable`
`validate-request-secret {enable | disable}`	Enable if you want FortiOS Carrier to verify that the RADIUS `secret` matches the RADIUS secret in the RADIUS Start or End record. You can verify the RADIUS secret to verify that the RADIUS record is valid.	`disable`
`vdom <vdom-name>`	Specify the VDOM that receives RADIUS packets and sends RADIUS packets. This should be the management VDOM.	root

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.

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`

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.

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 362.

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 339.

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 srv-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`
`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`

Variable	Description	Default
`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`
`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 636.	`disable`

Variable	Description	Default
`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 srv-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`.	`::`

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`

gi-gk

This command configures the settings for the FortiOS Carrier Gi gateway firewall. This firewall is used in the anti-overbilling configuration, and can be enabled on a per interface basis. For more information see "system interface" on page 381.

Syntax

```
config system gi-gk
  set context <id_integer>
  set port <tcp_port>
end
```

Variable	Description	Default
`context <id_integer>`	Enter the context ID for the Gi gateway firewall	
`port <tcp_port>`	Enter the TCP port to listen to. Valid range is from 0 to 65535.	0

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`.

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 {disable | strict}
  set clt-cert-req {enable | disable}
  set daily-restart {enable | disable}
  set detection-summary {enable | disable}
  set dst {enable | disable}
  set endpoint-control-fds-access {enable | disable}
  set endpoint-control-portal-port <endpoint_port>
  set failtime <failures_count>
  set fds-statistics {enable | disable}
  set fds-statistics-period <minutes>
  set fgd-alert-subscription {advisory latest-threat latest-virus
     latest-attack new-virus-db new-attack-db}
  set fortiswitch-heartbeat {enable | disable}
  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 ipsec-hmac-offload {disable | enable}
    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 revision-backup-on-logout {disable | enable}
    set remoteauthtimeout <timeout_sec>
    set reset-sessionless-tcp {enable | disable}
    set restart-time <hh:mm>
    set revision-backup-on-logout {enable | disable}
    set scanunit-count <count_int>
    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 409.	`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

Variable	Description	Default
`anti-replay {disable	loose	strict}`	Set the level of checking for packet replay and TCP sequence checking (or TCP Sequence (SYN) number checking). All TCP packets contain a Sequence Number (SYN) and an Acknowledgement Number (ACK). The TCP protocol uses these numbers for error free end-to-end communications. TCP sequence checking can also be used to validate individual packets. FortiGate units use TCP sequence checking to make sure that a packet is part of a TCP session. By default, if a packet is received with sequence numbers that fall out of the expected range, the FortiGate unit drops the packet. This is normally a desired behavior, since it means that the packet is invalid. But in some cases you may want to configure different levels of anti-replay checking if some of your network equipment uses non-RFC methods when sending packets. You can set anti-replay protection to the following settings: `disable` No anti-replay protection. `loose` Perform packet sequence checking and ICMP anti-replay checking with the following criteria: • The SYN, FIN, and RST bit can not appear in the same packet. • The FortiGate unit does not allow more than 1 ICMP error packet to go through the FortiGate unit before it receives a normal TCP or UDP packet. • If the FortiGate unit receives an RST packet, and `check-reset-range` is set to `strict` the FortiGate unit checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect. `strict` Performs all of the loose checking but for each new session also checks to determine of the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value for each new session. Strict anti-replay checking can also help prevent SYN flooding. If any packet fails a check it is dropped. If “other-traffic {disable | enable}” on page 177 is enabled a log message is written for each packet that fails a check.	`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`
`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`

Variable	Description	Default
`av-failopen {idledrop | off | one-shot | pass}`	Set the action to take if the unit is running low on memory or the proxy connection limit has been reached. Valid options are `idledrop`, `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.	`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`.	`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 618.	`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. • `manual` 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 621 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 621 for more information.	`600`
`check-reset-range {disable | strict}`	Configure ICMP error message verification. • `disable` the FortiGate unit does not validate ICMP error messages. • `strict` If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) | TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If "other-traffic {disable | enable}" on page 177 is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the `anti-replay` option checks packets.	`disable`

Variable	Description	Default
check-protocol-header {loose | strict}	Select the level of checking performed on protocol headers. • loose the FortiGate unit performs basic header checking to verify that a packet is part of a session and should be processed. Basic header checking includes verifying that the layer-4 protocol header length, the IP header length, the IP version, the IP checksum, IP options are correct, etc. • strict the FortiGate unit does the same checking as above plus it verifies that ESP packets have the correct sequence number, SPI, and data length. If the packet fails header checking it is dropped by the FortiGate unit and logged if "other-traffic {disable | enable}" on page 177 is enabled.	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
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-fds-access {enable | disable}	Enable or disable access to FortiGuard servers for non-compliant endpoints.	enable
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
fgd-alert-subscription {advisory latest-threat latest-virus latest-attack new-virus-db new-attack-db}	Select what to retrieve from FortiGuard: advisory — FortiGuard advisories, report and news alerts latest-attack — latest FortiGuard attack alerts latest-threat — latest FortiGuard threats alerts latest-virus — latest FortiGuard virus alerts new-antivirus-db — FortiGuard AV database release alerts new-attack-db — FortiGuard IPS database release alerts.	null
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
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

Variable	Description	Default
`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. Some models support hostnames 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`
`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.	`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
`ipsec-hmac-offload {disable | enable}`	Enable to offload IPsec HMAC processing to hardware or disable to not offload IPsec HMAC processing to hardware.	`enable`
`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`

Variable	Description	Default
`lcdpin <pin_number>`	Set the 6 digit PIN administrators must enter to use the LCD panel.	123456
`lcdprotection {enable | disable}`	Enable or disable LCD panel PIN protection.	`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`
`optimize {antivirus | throughput}`	Set firmware performance optimization to either `antivirus` or `throughput`.	`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`
`revision-backup-on-logout {disable | enable}`	Enable or disable backing up the latest configuration revision when the administrator logs out of the CLI or web-based manager.	`enable`
`remoteauthtimeout <timeout_sec>`	The number of seconds that the FortiGate unit waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. The range is 0 to 300 seconds, 0 means no timeout. To improve security keep the remote authentication timeout at the default value of 5 seconds. However, if a RADIUS request needs to traverse multiple hops or several RADIUS requests are made, the default timeout of 5 seconds may not be long enough to receive a response.	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`

Variable	Description	Default
`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.
`revision-backup-on-logout {enable | disable}`	Back up the current configuration on logout if it has changed since the last backup.	`enable`
`scanunit-count <count_int>`	Tune the number of scanunits. The range and default depend on the number of CPUs. Only available on FortiGate units with multiple CPUs. Recommended for advanced users.	`depends on the model`
`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.	`disable`
`sslvpn-sport <port_number>`	Enter the port to use for SSL VPN. SSL VPN users must browse to the FortiGate unit using this port to connect to an SSL VPN portal.	10443
`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`

Variable	Description	Default
`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 466. 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`
`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`

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, VLAN, or IPsec VPN 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.	

ha

Use this command to enable and configure FortiGate high availability (HA) and virtual clustering.

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 (`config system session-sync`).

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 ha-eth-type <type_int>
  set ha-mgmt-status {enable | disable}
  set ha-mgmt-interface <interface_name>
  set ha-mgmt-interface-gateway <gateway_interface>
  set hb-interval <interval_integer>
  set hb-lost-threshold <threshold_integer>
  set hbdev <interface_name> <priority_integer> [<interface_name>
     <priority_integer>]...
  set hbdev <interface_name> <priority_integer> [<interface_name>
     <priority_integer>]...
  set hc-eth-type <type_int>
  set helo-holddown <holddown_integer>
  set l2ep-eth-type <type_int>
  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 subsecond {enable | disable}
  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). The range is 1 to 60.	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 range is 1 to 20 seconds.	8
`authentication {disable | enable}`	Enable/disable HA heartbeat message authentication using SHA1.	`disable`
`encryption {disable | enable}`	Enable/disable HA heartbeat message encryption using AES-128 for encryption and SHA1 for authentication.	`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`
`ha-eth-type <type_int>`	Set the Ethertype used by HA heartbeat packets for NAT/Route mode clusters. `<type_int>` is a 4-digit number.	8890
`ha-mgmt-status {enable | disable}`	Enable or disable the HA reserved management interface feature.	`disable`
`ha-mgmt-interface <interface_name>`	Configure the FortiGate interface to be the reserved HA management interface. You can configure the IP address and other settings for this interface using the config system interface command. When you enable the reserved management interface feature the configuration of the reserved interface is not synchronized among cluster units.	No default.
`ha-mgmt-interface-gateway <gateway_interface>`	Configure the default route for the reserved HA management interface.	0.0.0.0
`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 range is 1 to 60 packets.	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.	2

Variable	Description	Default
`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. 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. 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.
`hc-eth-type <type_int>`	Set the Ethertype used by HA heartbeat packets for Transparent mode clusters. `<type_int>` is a 4-digit number.	8891
`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. The range is 5 to 300 seconds.	`20`
`l2ep-eth-type <type_int>`	Set the Ethertype used by HA telnet sessions between cluster units over the HA link. `<type_int>` is a 4-digit number.	8893
`link-failed-signal {disable | enable}`	Enable or disable shutting down all interfaces (except for heartbeat device interfaces) of a cluster unit with a failed monitored interface for one second after a failover occurs. Enable this option if the switch the cluster is connected to does not update its MAC forwarding tables after a failover caused by a link failure.	`disable`
`load-balance-all {disable | enable}`	Select the traffic that is load balanced by active-active HA. Enable to load balance TCP sessions and sessions for firewall policies that include UTM options. Disable to load balance only sessions for firewall policies that include UTM options. Available if `mode` is `a-a`.	`disable`
`mode {a-a | a-p | standalone}`	Set the HA mode. Enter `a-p` to create an Active-Passive cluster. Enter `a-a` to create an Active-Active cluster. Enter `standalone` to disable HA. 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`.	`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, IPSec VPN interfaces, or switch interfaces. You can monitor up to 16 interfaces. This limit only applies to FortiGate units with more than 16 physical interfaces. In a multiple VDOM configuration you can monitor up to 16 interfaces per virtual cluster.	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. Automatically changes to `enable` when you enable virtual cluster 2.	`disable`
`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.	No default

Variable	Description	Default
`pingserver-failover-threshold <threshold_integer>`	Set the HA remote IP monitoring failover threshold. 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. Set the priority for each remote IP monitoring ping server using the `ha-priority` field of the command "system interface" on page 381.	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.	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.	
`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.	10
`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. 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. • `ipport` load balancing according to IP address and port. • `leastconnection` least connection load balancing. • none no load balancing. Use none when the cluster interfaces are connected to load balancing switches. • `random` random load balancing. • `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 assign weighted values to each of the units in a cluster.	`round-robin`

Variable	Description	Default
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.	disable
subsecond {enable | disable}	Enable or disable subsecond failover. This feature can accelerate HA failover depending on the FortiGate unit hardware configuration and the network configuration. This option also changes how the FortiGate unit processes firmware upgrades to reduce service interruptions. The success of this feature depends on the FortiGate hardware configuration and the network configuration. Network devices that respond slowly to an HA failover can prevent this feature from reducing failover times to less than a second.	disable
sync-config {disable | enable}	Enable or disable automatic synchronization of primary unit configuration changes to all cluster units.	enable
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 16 FortiGate units so you can set up to 16 weights. The default weight means that the 16 possible units in the cluster all have the same weight of 1. The cluster units are numbered 0 to 15. priority_integer is a number from 0 to 16 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 0 5 set weight 1 10 set weight 2 15 set weight 3 20	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Variable	Description	Default
`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. When multiple VDOMs are enabled, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use `config secondary-vcluster` 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` `enable` when multiple VDOMs are enabled
`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`.

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 (some FortiGate models)” on page 398.

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 364.

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-auth {disable | tsig}
    set ddns-domain <ddns_domain_name>
    set ddns-key <key_str>
    set ddns-keyname <kname_str>
    set ddns-password <ddns_password>
    set ddns-server <ddns_service>
    set ddns-server-ip <ipv4_addr>
    set ddns-sn <ddns_sn>
    set ddns-ttl <ttl_int>
    set ddns-username <ddns_username>
    set ddns-zone <zone_name>
    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 external {enable | disable)
    set fail-detect {enable | disable}
    set fail-detect-option {link-down | detectserver}
    set fail-alert-method {link-down | link-failed-signal}
    set fail-alert-interfaces {port1 port2 ...}
    set forward-domain <collision_group_number>
    set fp-anomaly [...]
    set gi-gk {enable | disable}
    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 npu-fastpath {disable | enable}
    set padt-retry-timeout <padt_retry_seconds>
    set npu-fastpath {disable | enable}
    set password <pppoe_password>
    set peer-interface <interface>
    set poe {disable | enable}
    set polling-interval <interval_int>
    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 sample-direction {both | rx | tx}
    set sample-rate <rate_int>
    set sflow-sampler {disable | enable}
    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
      config ip6-extra-address
        edit <prefix_ipv6>
        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 vrrp
      edit <VRID>
        set adv-interval <seconds_int>
        set preempt {enable | disable}
        set priority <prio_int>
        set start-time <seconds_int>
        set status {enable | disable}
        set vrdst <ipv4_addr>
        set vrip <ipv4_addr>
      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
`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. Enabling this option may make the FortiGate unit vulnerable to broadcast-based DoS attacks such as ping floods.	`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-auth {disable | tsig}`	Enable TSIG authentication for the generic DDNS server.	`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-key <key_str>`	For TSIG authentication of generic DDNS server, enter the key.	
`ddns-keyname <kname_str>`	For TSIG authentication of generic DDNS server, enter the keyname.	

Variable	**Description**	**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-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. **dyndns.org** — supports members.dyndns.org. **dyns.net** — supports www.dyns.net. **genericDDNS —** supports DDNS server (RFC 2136) defined in ddns-server-ip **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-server-ip <ipv4_addr>`	Enter the DDNS server IP address for genericDDNS server.	0.0.0.0
`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-ttl <ttl_int>`	Enter the time-to-live value for DDNS packets.	300
`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.
`ddns-zone <zone_name>`	Enter a name for your DDNS zone. Available if `ddns-server` is `genericDDNS`.	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`
`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.

Variable	Description	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 296 This variable is only available in NAT/Route mode when `mode` is set to `dhcp` or `pppoe`.	5
`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 350. **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 some models 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`
`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.
`external {enable | disable)`	Enable to indicate that an interface is an external interface connected to an external network. This option is used for SIP NAT when the `config VoIP profile` SIP `contact-fixup` option is disabled.	`disable`
`explicit-web-proxy {enable | disable}`	Enable explicit Web proxy on this interface. For more information, see “explicit” on page 576.	`disable`

Variable	Description	Default
`fail-detect {enable | disable}`	Enable interface failure detection.	`disable`
`fail-detect-option {link-down | detectserver}`	Select whether the FortiGate unit detects interface failure by port detection (`link-down`) or ping server (`detectserver`).	`link-down`
`fail-alert-method {link-down | link-failed-signal}`	Select the signal that the FortiGate unit uses to signal the link failure: Link Down or Link Failed.	`link-down`
`fail-alert-interfaces {port1 port2 ...}`	Select the interfaces to which failure detection applies.	
`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.	`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.	`No options specified (disabled)`
`gi-gk {enable | disable}`	Enable FortiOS Carrier Gi Gatekeeper to enable the Gi firewall on this interface as part of the anti-overbilling configuration.	`disable`
`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 364.	`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 375. 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 86 and “ipmacbinding table” on page 87.	`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 131 and “firewall sniff-interface-policy6” on page 133.	`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.	`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. Some models 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 576. This variable is only available when this interface is in NAT/Route mode.	`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
`npu-fastpath {disable | enable}`	Disable to turn off NP2 fast path acceleration.	`enable`
`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

Variable	Description	Default
`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.
`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.	
`poe {disable | enable}`	Enable or disable PoE (Power over Ethernet). This option is only available on models with PoE feature.	`disable`
`polling-interval <interval_int>`	Set the amount of time in seconds that the sFlow agent waits between sending collected data to the sFlow collector. The range is 1 to 255 seconds. A higher `polling-interval` means less data is sent across the network but also means that the sFlow collector's picture of the network may be out of date.	20
`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 295. 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.
`sample-direction {both | rx | tx}`	Configure the sFlow agent to sample traffic received by the interface (`rx`) or sent from the interface (`tx`) or `both`.	`both`

Variable	Description	Default
`sample-rate <rate_int>`	Set the sample rate for the sFlow agent added to this interface. The sample rate defines the average number of packets to wait between samples. For example, the default `sample-rate` of 2000 samples 1 of every 2000 packets. The `sample-rate` range is 10 to 99999 packets between samples. The lower the `sample-rate` the higher the number of packets sampled. Sampling more packets increases the accuracy of the sampling data but also increases the CPU and network bandwidth required to support sFlow. The default `sample-rate` of 2000 provides high enough accuracy in most cases. You can increase the `sample-rate` to reduce accuracy. You can also reduce the `sample-rate` to increase accuracy.	2000
`sflow-sampler {disable | enable}`	Add an sFlow agent to an interface. You can also configure the sFlow agent's `sample-rate`, `polling-interval`, and `sample-direction`. You can add sFlow agents to any FortiGate interface, including physical interfaces, VLAN interfaces, and aggregate interfaces. After adding the sFlow agent you can configure the sFlow For more information about sFlow see "system sflow" on page 457.	`disable`
`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 switch interfaces.	`auto`
`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`

Variable	Description	Default
`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.
`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 some FortiGate models. 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 (some FortiGate models)" on page 398. **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 465. **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 468. **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 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.

Variable	Description	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.	root
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.	No default.
wccp {enable | disable}	Enable to WCCP on an interface. This setting specifies the interface the FortiGate unit sends and receives WCCP packets and redirected traffic.	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 to FortiWiFi units 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.

Variable	Description	Default
`wifi-mac-filter {enable | disable}`	Enable MAC filtering for the wireless interface.	`disable`
`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 ip6-extra-addr`	Configure a secondary address for this IPv6 interface.	
`<prefix_ipv6>`	IPv6 address prefix.	
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

Variable	Description	Default
`password <password>`	Enter the password for L2TP.	n/a
`peer-host <ipv4_addr>`	Enter the IP address of the L2TP host.	n/a
`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 (some FortiGate models) **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`
`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 when `type` is `aggregate`.	`slow`

Variable	Description	Default

`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.

`config vrrp` **fields**		
`<VRID>`	Router ID	

`adv-interval`
`<seconds_int>`
	Advertisement interval (1-255 seconds).	1

`preempt`
`{enable | disable}`
	Enable or disable preempt mode.	`enable`

`priority <prio_int>`	Priority of the virtual router (1-255).	100
`start-time <seconds_int>`	Startup time (1-255 seconds).	3

`status`
`{enable | disable}`
	Enable or disable this router.	`enable`

`vrdst <ipv4_addr>`	Monitor the route to this destination.	`0.0.0.0`
`vrip <ipv4_addr>`	IP address of the virtual router.	`0.0.0.0`

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

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.

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.

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`

Variable	Description	Default

`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 296. 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`
`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`.	`generic`

Variable	Description	Default
`peer_modem2 {actiontec | ascendTNT | generic}`	If the modem at `phone2` is Actiontec or AscendTNT, select that type, otherwise leave setting as `generic`.	`generic`
`peer_modem3 {actiontec | ascendTNT | generic}`	If the modem at `phone3` is Actiontec or AscendTNT, select that type, otherwise leave setting as `generic`.	`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 295.	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.

`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`

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`

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 ntpv3 {enable | disable}
      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	
`ntpv3 {enable | disable}`	Use NTPv3 protocol instead of NTPv4.	`disable`
`server <IPv4_addr>[/<hostname_str>`	Enter the IPv4 address and hostname (optional) for this NTP server.	

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`

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.

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 3: 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.

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 327.

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 4.	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 4: alertmail message types

Message Type	Description
`alertmail-block`	*Virus detected* must be enabled for alert email. Antivirus *File Filter* must be enabled in an antivirus 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 327.
`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 an antivirus 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 5: 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.

replacemsg auth

The FortiGate unit uses the text of the authentication replacement messages listed in Table 7 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.

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 6 on page 413.	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 6: 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 7: 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>`

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 8: 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.

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 9 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 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 9.	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 9: FortiGuard Web Filtering replacement messages

Message name	Description
`ftgd-block`	*Enable FortiGuard Web Filtering* is enabled in a web filter 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 589. 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 web filter profile for HTTP or HTTPS, and blocks a web page. The blocked page is replaced with the `http-err` web page.

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 10.	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 10: FTP replacement messages

Message name	Description
`ftp-dl-blocked`	Antivirus *File Filter* enabled for FTP in an antivirus 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 an antivirus 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 an antivirus 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 11: 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.

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 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 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.

Table 12: HTTP replacement messages

Message name	Description
`bannedword`	Web content blocking is enabled in a web filter 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 web filter 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 web filter 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 an antivirus 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 an antivirus 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 12: HTTP replacement messages

Message name	Description
`http-client-filesize`	*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`	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 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* 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. 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 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 104.
`url-block`	Web URL filtering is enabled 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 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
`%%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.

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 14.	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: 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 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 deletes an infected file from and replaces the file with this message.
`im-file-xfer-name`	Antivirus *File Filter* enabled for IM 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 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. 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. 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!.

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
`%%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.

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 16.	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 16: mail message types

Message name	Description
`email-block`	The antivirus *File Filter* is enabled for an email protocol 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 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 deletes an infected file from an email message and replaces the file with the `email-virus` message.
`partial`	Antivirus *Pass Fragmented Emails* is not enabled so a fragmented email is blocked. The `partial` message replaces the first fragment of the fragmented email.

Table 16: mail message types

Message name	Description
`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 17: 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.

replacemsg mm1

Use this command to change default replacement messages added to messages sent by FortiOS Carrier on the MM1 network 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.

Syntax

```
config system replacemsg mm1 <message_type>
  set add-smil {enable | disable}
  set charset <character_set>
  set class <class>
  set format <format>
  set from <from_address>
  set from-sender {enable | disable}
  set header <header_type>
  set image <string>
  set message <message_text>
  set priority <priority>
  set rsp-status <rsp_status>
  set rsp-text <response_text>
  set sender-visibility <sender_vis>
  set smil-part <string>
  set subject <subject_text>
end
```

Variable	Description	Default
`<message_type>`	MM1 replacement message types, one of: **mm1-retr-conf-block** **mm1-retr-conf-bword** **mm1-retr-conf-sis-block** **mm1-retr-conf-virus** **mm1-send-conf-block** **mm1-send-conf-bword** **mm1-send-conf-sis-block** **mm1-send-conf-virus** **mm1-send-req-block** **mm1-send-req-bword** **mm1-send-req-sis-block** **mm1-send-req-virus**	No default.
`add-smil {enable | disable}`	Enable to add SMIL content to the message. SMIL content can include images. This field is available for the following message types: **mm1-send-req-block** **mm1-send-req-bword** **mm1-send-req-sis-block** **mm1-send-req-virus**	`disable`
`charset <character_set>`	Character encoding used for replacement message, one of: **us-ascii** **utf-8**	`utf-8`

`class <class>`	The message can be classified as one of: **advertisement** **automatic** **informational** **not-included** **personal**	`automatic`
`format <format>`	Set the format of the message, one of: **html** **none** **text** **wml** Not all formats are supported by all message types.	`text`
`from <from_address>`	Address the message is from.	`null`
`from-sender {enable | disable}`	Enable for the notification message to be sent from the recipient. This is to avoid billing problems.	`disable`
`header <header_type>`	Set the format of the message header, one of: **8bit** **http** **none**	`http`
`image <string>`	Enter the name of the image to include in the SMIL message part. Using '?' will show the list of available image names. This is only available when add-smil is enabled.	
`message <message_text>`	Text of the replacement message.	Depends on message type.
`priority <priority>`	Priority of the message, one of: **high** **low** **normal** **not included**	`normal`
`rsp-status <rsp_status>`	Response status code, one of: **err-content-not-accepted** **err-msg-fmt-corrupt** **err-msg-not-found** **err-net-prob** **err-snd-addr-unresolv** **err-srv-denied** **err-unspecified** **err-unsupp-msg** **ok**	`err-content-not-accepted`
`rsp-text <response_text>`	Response text.	Depends on message type.
`sender-visibility <sender_vis>`	Sender visibility, one of: **hide** **not-specified** **show**	`not-specified`
`smil-part <string>`	Enter the SMIL part of the replacement message.	
`subject <subject_text>`	Subject text string.	Depends on message type.

replacemsg mm3

Use this command to change default replacement messages added to messages sent by FortiOS Carrier on the MM3 network 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.

Syntax

```
config system replacemsg mm3 <message_type>
  set charset <character_set>
  set format <format>
  set from <from_address>
  set header <header_type>
  set message <message_text>
  set priority <priority>
  set subject <subject_text>
end
```

Variable	Description	Default
`<message_type>`	MM3 replacement message types, one of: **mm3-block** **mm3-block-notif** **mm3-bword** **mm3-bword-notif** **mm3-sis-block** **mm3-sis-block-notif** **mm3-sis-block-notif** **mm3-virus** **mm3-virus-block**	No default
`charset <character_set>`	Character encoding used for replacement messages, one of: **us-ascii** **utf-8**	`utf-8`
`format <format>`	Replacement message format flag, one of: **html** **none** **text** **wml**	`text`
`from <from_address>`	Address the message is from.	`null`
`header <header_type>`	Set the format of the message header, one of: **8bit** **http** **none**	`none`
`message <message_text>`	Text of the replacement message.	Depends on message type.
`priority <priority>`	Priority of the message, one of: **high** **low** **normal** **not included**	`normal`
`subject <subject_text>`	Subject text string.	Depends on message type.

replacemsg mm4

Use this command to change default replacement messages added to messages sent by FortiOS Carrier on the MM4 network 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.

Syntax

```
config system replacemsg mm4 <message_type>
  set charset <character_set>
  set class <class>
  set domain <address_domain>
  set format <format>
  set from <from_address>
  set from-sender {enable | disable}
  set header <header_type>
  set image <string>
  set message <message_text>
  set priority <priority>
  set rsp-status <rsp_status>
  set smil-part <string>
  set subject <subject_text>
end
```

Variable	Description	Default
`<message_type>`	MM4 replacement message types, one of: **mm4-block** **mm4-block-notif** **mm4-bword** **mm4-bword-notif** **mm4-sis-block** **mm4-sis-block-notif** **mm4-virus** **mm4-virus-block**	No default
`add-smil {enable | disable}`	Enable to add SMIL content to the message. SMIL content can include images. This field is available for the following message types: **mm4-block-notif** **mm4-bword-notif** **mm4-sis-block-notif**	`disable`
`charset <character_set>`	Character encoding used for replacement messages, one of: **us-ascii** **utf-8**	`utf-8`
`class <class>`	The message can be classified as one of: **advertisement** **automatic** **informational** **not-included** **personal**	`automatic`
`domain <address_domain>`	The from address domain.	null

`format <format>`	Replacement message format flag, one of: **html** **none** **text** **wml**	`text`
`from <from_address>`	Address the message is from.	`null`
`from-sender {enable | disable}`	Enable for the notification message to be sent from the recipient. This is to avoid billing problems.	`disable`
`header <header_type>`	Set the format of the message header, one of: **8bit** **http** **none**	`none`
`image <string>`	Enter the name of the image to include in the SMIL message part. Using '?' will show the list of available image names. This is only available when add-smil is enabled.	
`message <message_text>`	Text of the replacement message.	Depends on message type.
`priority <priority>`	Priority of the message, one of: **high** **low** **normal** **not included**	`normal`
`rsp-status <rsp_status>`	Response status codes, one of: **err-content-not-accepted** **err-msg-fmt-corrupt** **err-net-prob** **err-snd-addr-unresolv** **err-srv-denied** **err-unspecified** **err-unsupp-msg** **ok**	`err-content-not-accepted`
`smil-part <string>`	Enter the SMIL part of the replacement message.	
`subject <subject_text>`	Subject text string.	Depends on message type.

replacemsg mm7

Use this command to change default replacement messages added to messages sent by FortiOS Carrier on the MM7 network 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.

Syntax

```
config system replacemsg mm7 <mm7message_type>
  set add-smil {enable | disable}
  set addr_type <addr_type>
  set charset <character_set>
  set class <class>
  set format <format>
  set from <from_address>
  set from-sender {enable | disable}
  set header <header_type>
  set image <string>
  set message <message_text>
  set priority <priority>
  set rsp-status <rsp_status>
  set smil-part <string>
  set subject <subject_text>
end
```

Variable	Description	Default
`<mm7message_type>`	MM7 replacement message types, one of: **mm7-block** **mm7-block-notif** **mm7-bword** **mm7-bword-notif** **mm7-sis-block** **mm7-sis-block-notif** **mm7-virus** **mm7-virus-block**	No default
`add-smil {enable | disable}`	Enable to add SMIL content to the message. SMIL content can include images. This field is available for the following message types: **mm7-block-notif** **mm7-bword-notif** **mm7-sis-block-notif**	`disable`
`addr_type <addr_type>`	From address types, one of: **number** **rfc2882-addr** **short-code**	`number`
`charset <character_set>`	Character encoding used for replacement messages, one of: **us-ascii** **utf-8**	`utf-8`
`class <class>`	The message can be classified as one of: **advertisement** **automatic** **informational** **not-included** **personal**	`automatic`

`format <format>`	Replacement message format flag, one of: **html** **none** **text** **wml**	`text`
`from <from_address>`	Address the message is from.	`null`
`from-sender {enable | disable}`	Enable for the notification message to be sent from the recipient. This is to avoid billing problems.	`disable`
`header <header_type>`	Set the format of the message header, one of: **8bit** **http** **none**	`none`
`image <string>`	Enter the name of the image to include in the SMIL message part. Using '?' will show the list of available image names. This is only available when add-smil is enabled.	
`message <message_text>`	Text of the replacement message.	Depends on message type.
`priority <priority>`	Priority of the message, one of: **high** **low** **normal** **not included**	`normal`
`rsp-status <rsp_status>`	Response status codes, one of: **addr-err** **addr-not-found** **app-addr-not-supp** **app-denied** **app-id-not-found** **client-err** **content-refused** **gen-service-err** **improper-ident** **link-id-not-found** **msg-fmt-corrupt** **msg-id-not-found** **msg-rejected** **multiple-addr-not-supp** **not-possible** **oper-restrict** **partial-success** **repl-app-id-not-found** **service-denied** **service-err** **service-unavail** **srv-err** **success** **unsupp-oper** **unsupp-ver** **validation-err**	Depends on message type.
`smil-part <string>`	Enter the SMIL part of the replacement message.	
`subject <subject_text>`	Subject text string.	Depends on message type.

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

replacemsg-group

In FortiOS Carrier, replacement messages can be created and applied to specific profile groups. This allows the customization of messages for specific users or user groups.

If a user is not part of a custom replacement message group, their replacement messages come from the ‘default’ group. The ‘default’ group always exists, and cannot be deleted. All additional replacement message groups inherit from the default group. Any messages in custom groups that have not been modified, inherit any changes to those messages in the default group.

The only replacement messages that can not be customized in groups are administration related messages, which in the following categories:

- Alert Mail
- Administration
- Authentication
- IM and P2P
- SSL VPN

Except for mm1, mm3, mm4, mm7 which use the `message` field, all replacement message types use the `buffer` field to refer to the body of the message.

Syntax

```
config system replacemsg_group
  edit <groupname_string>
    set comment <string>
    config {fortiguard-wf | ftp | http | mail | mm1 | mm3 | mm4 | mm7 |
       nntp | spam}
      edit <msgkey_integer>
        set msg-type <type>
        set buffer <string>
        set header <header_flag>
        set format <format_flag>
        set message <string>
      end
  end
```

Variable	Description	Default
`edit <groupname_string>`	Create or edit a replacement message group.	
`comment <string>`	Enter a descriptive comment for this replacement message group.	
`config {fortiguard-wf	ftp	http	mail	mm1	mm3	mm4	mm7	nntp	spam}`	Select a replacement message type to add or edit. These types or protocols, match with the existing replacemsg commands, and determine which msg-types are available. For more information on these replacement message types see: • “replacemsg fortiguard-wf” on page 417 • “replacemsg ftp” on page 418 • “replacemsg http” on page 420 • “replacemsg mail” on page 424 • “replacemsg mm1” on page 426 • “replacemsg mm3” on page 428 • “replacemsg mm4” on page 429 • “replacemsg mm7” on page 431 • “replacemsg nntp” on page 438 • “replacemsg spam” on page 440	

	Variable	Description	Default
`edit <msgkey_integer>`		Create or edit a message entry in the table. Enter the key of the entry. Using '?' will show you the existing message type as well as the msgkey entries in the table.	
	`msg-type <type>`	Select the message type for this message entry. Valid message types vary according to which replacement message table you are editing. For a list of valid message types for this table, refer to the CLI replacemsg command of the same name.	
	`buffer <string>`	Enter the replacement message for this message type. Enclose the message in quotes. This field is used with the following replacement messages: **fortiguard-wf** **ftp** **http** **mail** **nntp** **spam** Other replacement messages use the `message` field.	
	`header <header_flag>`	Select the header for this message. Valid types include: **8bit** **http** **none**	
	`format <format_flag>`	Select the format of this message. Valid formats include: **html** **none** **text** **wml**	
	`message <string>`	Enter the replacement message for this message type. Enclose the message in quotes. This field is used with the following replacement messages: **mm1** **mm3** **mm4** **mm7** Other replacement messages use the `buffer` field.	

replacemsg-image

Use this command to add, edit, or delete images to be used in SMIL parts of FortiOS Carrier replacement messages. Both image-base64 and image-type must be present for a valid entry.

Syntax

```
config system replacemsg-image
  edit <image_name>
    set image-base64 <image_data>
    set image-type <format>
  end
```

Variable	**Description**	**Default**
`edit <image_name>`	Enter the name or tag to use for this image	none.
`image-base64 <image_data>`	Enter the image in base64 encoding. You can also use the graphical interface to add images by browsing to their location.	none.
`image-type <format>`	Select the format of the image. Available formats include: **gif** **jpeg** **png** **tiff**	none.

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 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: 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 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 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* 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.

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 19.	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 19: net news transfer protocol (NNTP) message types

Message name	Description
`nntp-dl-blocked`	Antivirus *File Filter* is enabled for NNTP 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. 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 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 20: 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

replacemsg spam

The FortiGate unit adds the Spam replacement messages listed in Table 21 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 21.	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 21: spam message types

Message name	Description
`ipblocklist`	Spam Filtering *IP address BWL check* enabled for an email protocol identifies an email message as spam and adds this replacement message.
`reversedns`	Spam Filtering *Return e-mail DNS check* enabled for an email protocol 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 identifies an email message as spam and adds this replacement message.
`smtp-spam-dnsbl`	From the CLI, `spamrbl` enabled for an email protocol 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 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 identifies an email message as spam and adds this replacement message.

Table 21: spam message types

Message name	Description
`submit`	Any Spam Filtering option enabled for an email protocol 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 22: 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.

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.

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.

replacemsg webproxy

The web proxy returns messages for user authentication failures and HTTP errors.

Syntax

```
config system replacemsg webproxy {auth-authorization | auth-challenge
   | auth-login | deny | http-err | user-limit}
  set buffer <message>
  set format <format>
  set header <header_type>
```

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**	`html`
`header <header_type>`	Set the format of the message header: **8bit** **http** **none**	`http`

The `http-err` replacement message requires the following tags:

Table 23: Web proxy http-err replacement message tags

Tag	Description
%%HTTP_ERR_CODE%%	The returned HTTP error code, “404” for example.
%%HTTP_ERR_DESC%%	The returned HTTP error message, “Not Found” for example.
%%PROTOCOL%%	The protocol that applies to the traffic, “http://” for example.
%%URL%%	The URL (not including protocol) that caused the error.

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 469.

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 ipsec-phase1 <max_int>
    set ipsec-phase2 <max_int>
    set log-disk-quota <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>
    set web-proxy <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.	
`ipsec-phase1 <max_int>`	Enter the maximum number of IPSec phase1 tunnels.	
`ipsec-phase2 <max_int>`	Enter the maximum number of IPSec phase2 tunnels.	
`log-disk-quota <max_int>`	Enter the maximum amount of log disk space available in MBytes for global log messages. The range depends on the amount of hard disk space available.	
`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.	
`web-proxy <max_int>`	Enter the maximum number of users that can be using the explicit web proxy at one time. How the number of concurrent explicit proxy users is determined depends on their authentication method: • For session-based authenticated users, each authenticated user is counted as a single user. Since multiple users can have the same user name, the proxy attempts to identify users according to their authentication membership (based upon whether they were authenticated using RADIUS, LADAP, FSAE, local database etc.). If a user of one session has the same name and membership as a user of another session, the explicit proxy assumes this is one user. • For IP Based authentication, or no authentication, or if no web-proxy firewall policy has been added, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.	

session-helper

FortiGate units use session helpers to process sessions that have special requirements. Session helpers function like proxies by getting information from the session and performing support functions required by the session. For example:

- The SIP session helper looks inside SIP messages and performs NAT (if required) on the IP addresses in the SIP message and opens pinholes to allow media traffic associated with the SIP session to pass through the FortiGate unit.
- The FTP session helper can keep track of multiple connections initiated from a single FTP session. The session helper can also permits an FTP server to actively open a connection back to a client program.
- The TNS session helper sniffs the return packet from an initial 1521 SQLNET exchange and then uses the port and session information uncovered in that return TNS redirect packet to add a temporary firewall policy that accepts the new port and IP address supplied as part of the TNS redirect.

The session helper configuration binds a session helper to a TCP or UDP port and protocol. When a session is accepted by a firewall policy on that port and protocol the FortiGate unit passes the session to the session helper configured with this command. The session is processed by the session helper.

If your FortiGate unit accepts sessions that require a session helper on different ports than those defined by the session-helper configuration, then you can add more entire to the session helper configuration. Its OK to have multiple session helper configurations for a given protocol because only the matching configuration is used.

Use the `show system session` command to view the current session helper configuration.

FortiGate units include the session helpers listed in Table 24:

Table 24: FortiGate session helpers

Session helper name	Description
dcerpc	Distributed computing environment / remote procedure calls protocol (DCE/RPC).
dns-tcp	Domain name service (DNS) using the TCP protocol.
dns-udp	Domain name service (DNS) using the UDP protocol.
ftp	File transfer protocol (FTP).
h245I	H.245 I call-in protocol.
h245O	H.256 O call-out protocol.
h323	H.323 protocol.
mgcp	Media gateway control protocol (MGCP).
mms	Multimedia message service (MMS) protocol
pmap	Port mapper (PMAP) protocol.
pptp	Point to point tunneling protocol (PPTP).
ras	Remote access service (RAS) protocol.
rsh	Remote shell protocol (RSH).
sip	Session initiation protocol (SIP).
tftp	Trivial file transfer protocol (TFTP).
tns	Oracle transparent network substrate protocol (TNS or SQLNET).

Syntax

```
config system session-helper
  edit <helper-number>
```

```
        set name {dcerpc | dns-tcp | dns-udp | ftp | h245I | H2450 | h323 | mgcp
           | mms | pmap | pptp | ras | rsh | sip | tftp | tns}
        set port <port_number>
        set protocol <protocol_number>
    end
```

Variable	Description	Default
`<helper-number>`	Enter the number of the session-helper that you want to edit, or enter an unused number or 0 to create a new session-helper.	No default.
`name {dcerpc | dns-tcp | dns-udp | ftp | h245I | H2450 | h323 | mgcp | mms | pmap | pptp | ras | rsh | sip | tftp | tns}`	The name of the session helper to configure.	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.

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.

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.	

Variable	Description	Default
`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)

session-ttl

Use this command to configure port-range based session timeouts by setting the session time to live (ttl) for multiple TCP, UDP, or SCTP port number ranges. The session ttl is the length of time a TCP, UDP, or SCTP 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, UDP, or SCTP) 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, to 17 for UDP sessions, or to 132 for SCTP 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 1 - 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`

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 25: 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.

Note: When asymmetric routing is enabled, through the use of asymroute variable, the FortiGate unit can no longer perform stateful inspection.

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 {disable | enable}
  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>
    set wccp-cache-engine {enable | disable}
  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. **Note:** Enabling asymmetric routing disables stateful inspection. Your FortiGate unit can only perform stateless inspection in this state.	`disable`
`asymroute6 {enable | disable}`	Enable to turn on IPv6 asymmetric routing on your FortiGate unit, or this VDOM if you have VDOMs enabled.	`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.

Variable	Description	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.
`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`.	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 {disable | enable}`	Enable or disable the SIP session helper. The SIP session helper will process SIP sessions unless the SIP sessions are accepted by the SIP ALG.	`enable`
`sip-nat-trace {enable | disable}`	Select enable to record the original IP address of the phone.	`enable`
`sip-tcp-port <port_number>`	Enter the port number from 1 to 65535 that the SIP ALG monitors for SIP TCP sessions.	`5060`
`sip-udp-port <port_number>`	Enter the port number from 1 to 65535 that the SIP ALG monitors for SIP UDP sessions.	`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 295. **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 381.	`source-ip-based`
`vpn-stats-log {ipsec | l2tp | pptp | ssl}`	Enable periodic VPN log statistics for one or more types of VPN.	
`vpn-stats-period <period_int>`	Enter the interval in seconds for `vpn-stats-log` to collect statistics.	0
`wccp-cache-engine {enable | disable}`	Configure the FortiGate unit to operate as a WCCP cache engine. Use the `config system wccp` command to configure WCCP cache engine settings.	`disable`

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

sflow

Use this command to add or change the IP address and UDP port that FortiGate sFlow agents use to send sFlow datagrams to an sFlow collector.

sFlow is a network monitoring protocol defined in RFC 3176 and described in http://www.sflow.org. You can configure one or more FortiGate interfaces as sFlow agents that monitor network traffic and send sFlow datagrams containing information about traffic flow to an sFlow collector.

sFlow is normally used to provide an overall traffic flow picture of your network. You would usually operate sFlow agents on switches, routers, and firewall on your network, collect traffic data from all of them and use a collector to show traffic flows and patterns.

Syntax

```
config system sflow
  set collector-ip <collector_ipv4>
  set collector_port <port_int>
end
```

Variable	Description	Default
`collector-ip <collector_ipv4>`	The IP address of the sFlow collector that sFlow agents should send sFlow datagrams to.	0.0.0.0
`collector_port <port_int>`	The UDP port number used for sending sFlow datagrams. Change this setting only if required by your sFlow collector or you network configuration.	6343

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.

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 ha-direct {enable | disable}
      set interface <if_name>
      set ip <address_ipv4>
      set source-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 364. **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.	
`ha-direct {enable | disable}`	Enable direct management of cluster members.	`disable`
`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
`source-ip <address_ipv4>`	Enter the source IP address for SNMP traps sent by the FortiGate unit.	0.0.0.0

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.

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

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.

Syntax

```
config system snmp user
  edit <username>
    set auth-proto {md5 | sha}
    set auth-pwd <password>
    set events <event_string>
    set ha-direct {enable | disable}
    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.

Variable	Description	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 **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	No default
`ha-direct {enable | disable}`	Enable direct management of cluster members.	`disable`
`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`

storage

Use this command to add and edit local disk storage settings.

Syntax

```
config system storage
  edit <storage_name>
    set media-type <name>
    set partition <partition_ref_int>
  end
```

Variable	Description	Default
`<storage_name>`	The name for this storage.	
`media-type <name>`	The type of disk. You cannot configure or change this setting.	
`partition <partition_ref_int>`	The partition reference number. See "execute disk" on page 627.	

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. For more information on switch-mode, see “global” on page 364.

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)	`switch`
`vdom <vdom_name>`	Enter the VDOM to which the switch belongs.	No default.

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 270.

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`

vdom-dns

Use this command to configure DNS servers for a non-management VDOM. This command is only available from a non-management VDOM

DNS settings such as `dns-cache-limit` and set globally. See "system dns" on page 349.

Syntax

```
config system dns
  set ip6-primary <dns_ipv6>
  set ip6-secondary <dns_ip6>
  set primary <dns_ipv4>
  set secondary <dns_ip4>
  set vdom-dns {disable | enable}
end
```

Variable	Description	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.	`0.0.0.0`
`secondary <dns_ip4>`	Enter the secondary DNS IP server address.	`0.0.0.0`
`vdom-dns {disable | enable}`	Enable configuring DNS servers for the current VDOM.	`disable`

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.

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.	

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 445 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 log-disk-quota <max_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>]
      set web-proxy <max_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
`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
`log-disk-quota <max_int>`	Enter the maximum amount of log disk space available in MBytes for log messages for this VDOM. The range depends on the amount of hard disk space available.	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
`web-proxy <max_int>`	Enter the maximum number of users that can be using the explicit web proxy at one time from this VDOM. How the number of concurrent explicit proxy users is determined depends on their authentication method: • For session-based authenticated users, each authenticated user is counted as a single user. Since multiple users can have the same user name, the proxy attempts to identify users according to their authentication membership (based upon whether they were authenticated using RADIUS, LADAP, FSAE, local database etc.). If a user of one session has the same name and membership as a user of another session, the explicit proxy assumes this is one user. • For IP Based authentication, or no authentication, or if no web-proxy firewall policy has been added, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.	0 0

vdom-sflow

Use this command to add or change the IP address and UDP port that FortiGate sFlow agents operating on interfaces in a non-management VDOM use to send sFlow datagrams to an sFlow collector.

Syntax

```
config system sit-tunnel
  set collector-ip <collector_ipv4>
  set collector-ip <collector_ipv4>
  set vdom-sflow {disable | enable}
end
```

Variable	Description	Default
`collector-ip <collector_ipv4>`	The IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM should send sFlow datagrams to.	0.0.0.0
`collector_port <port_int>`	The UDP port number used for sending sFlow datagrams. Change this setting only if required by your sFlow collector or you network configuration.	6343
`vdom-sflow {disable | enable}`	Enable configuring sFlow settings for the current VDOM.	`enable`

wccp

Configure settings for Web Cache Communication Protocol (WCCP).

You can configure a FortiGate unit to operate as a WCCP router or client.

- A FortiGate unit operating as a WCCP router can intercept HTTP and HTTPS sessions and forward them to a web caching engine that caches web pages and returns cached content to the web browser.
- A FortiGate unit operating as a WCCP client can accept and forward WCCP sessions and use firewall policies to apply NAT, UTM, and other FortiGate security features to them. A FortiGate unit operates as a WCCP client only in NAT/Route mode (and not in Transparent mode)

Enter the following command to configure a FortiGate unit to operate as a WCCP router (this is the default FortiGate WCCP configuration):

```
config system settings
  set wccp-cache-engine disable
end
```

Enter the following command to configure a FortiGate unit to operate as a WCCP client:

```
config system settings
  set wccp-cache-engine enable
end
```

When you enter this command an interface named `w.<vdom_name>` is added to the FortiGate configuration (for example `w.root`). All WCCP sessions received by a FortiGate unit operating as a WCCP client are considered to be received at this interface and you can enter firewall policies for the WCCP traffic.

Syntax (WCCP router mode)

```
config system wccp
  edit <service-id>
    set router-id <interface_ipv4>
    set group-address <multicast_ipv4>
    set server-list <router_ipv4>
    set authentication {disable | enable}
    set forward-method {GRE | L2 | any}
    set return-method {GRE | L2 | any}
    set assignment-method {HASH | MASK | any}
    set password <password_str>
  next
end
```

Syntax (WCCP client mode)

```
config system wccp
  edit <service-id>
    set cache-id <cache_engine_ip4>
    set group-address <multicast_ipv4>
    set router-list <server_ipv4mask>
    set authentication {disable | enable}
    set service-type {auto | dynamic | standard}
    set assignment-weight <weight_int>
    set assignment-bucket-format {cisco-implementation | wccp-v2}
    set password <password_str>
  next
end
```

Variable	Description	Default
`<service-id>`	Valid ID range is from 0 to 255. 0 for HTTP.	`1`
`router-id <interface_ipv4>`	An IP address known to all cache engines. This IP address identifies a FortiGate interface IP address to the cache engines. If all cache engines 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 engines 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 engines that connect to that interface.	`0.0.0.0`
`cache-id <cache_engine_ip4>`	The IP address of the cache engine if its IP address is not the same as the IP address of a FortiGate interface. If the IP address of the cache engine is the same as the IP address of the FortiGate interface on which you have enabled WCCP, the `cache-id` should be 0.0.0.0.	`0.0.0.0`
`group-address <multicast_ipv4>`	The IP multicast address used by the cache routers. `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`
`server-list <router_ipv4>`	The IP address and net mask of the WCCP router.	`0.0.0.0 0.0.0.0`
`router-list <server_ipv4mask>`	IP addresses of one or more WCCP routers that can communicate with a FortiGate unit operating as a WCCP cache engine. Separate multiple addresses with a space.	
`authentication {disable | enable}`	Enable or disable using use MD5 authentication for the WCCP configuration.	`disable`
`service-type {auto | dynamic | standard}`	Set the WCCP service type used by the cache server.	`auto`
`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`
`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`
`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`
`assignment-weight <weight_int>`	Set the assignment weight for the WCCP cache engine. The range is 0 to 255.	`0`
`assignment-bucket-format {cisco-implementation | wccp-v2}`	Set the assignment bucket format for the WCCP cache engine.	`cisco-implementation`
`password <password_str>`	The authentication password. Maximum length is 8 characters.	No default.

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 475.

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`

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

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`

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 493.
   - See “user ldap” on page 487.
   - See “user tacacs+” on page 496
   - For Directory Service, see “user fsae” on page 485.
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 489.
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 486.
   - For Directory Service, also see “user ban” on page 481.

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 508.
2. Enter the certificate information for each VPN client (peer).
   - See “user peer” on page 490.
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 492.

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

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.

group

Use this command to add or edit user groups.

Syntax

```
config user group
  edit <groupname>
    set authtimeout <timeout>
    set group-type <grp_type>
    set member <names>
    set sslvpn-portal <web_portal_name>
    set ftgd-wf-ovrd-cookie {allow | deny}
    config match
      edit <match_id>
        set group-name <gname_str>
        set server-name <srvname_str>
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	`firewall`
`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.
`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.
config match fields	Specify the user group names on the authentication servers that are members of this FortiGate user group. If no matches are specified, all users on the server can authenticate.	
`<match_id>`	Enter an ID for the entry.	
`group-name <gname_str>`	The name of the matching group on the remote authentication server.	
`server-name <srvname_str>`	The name of the remote authentication server.	
`ftgd-wf-ovrd-cookie {allow | deny}`	Allow or deny this group browser cookie-based FortiGuard Web Filtering overrides for FortiOS Carrier. See "webfilter cookie-ovrd" on page 585.	`deny`

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 password-expiry-warning {disable | enable}
    set password-renewal {disable | enable}
    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.
`password-expiry-warning {disable | enable}`	Enable or disable password expiry warnings.	`disable`
`password-renewal {disable | enable}`	Enable or disable online password renewal.	`disable`
`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

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 487. 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 493. 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 496. 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.

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 web-based manager, 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`

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.

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, nas-ip`, and the `config user group` subcommand `config match`. 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-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.
`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

Variable	Description	Default
`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

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`

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.

voip

Use VoIP commands to configure VoIP profiles for firewall policies.

This chapter describes the following command:

profile

Use this command to add VoIP profiles for SIP, SIMPLE, and SCCP. To apply the SIP ALG, you add a VoIP profile to a firewall policy that accepts SIP sessions. All SIP sessions accepted by the firewall policy will be processed by the SIP ALG using the settings in the VoIP profile. The VoIP profile contains settings that are applied to SIP, Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) and Skinny Call Control Protocol (SCCP) sessions. You configure SIP and SCCP settings separately. SIP settings also apply to SIMPLE sessions.

Syntax

```
config voip profile
  edit <profile_name>
    set comment <comment_str>
    config sip
      set status {disable | enable}
      set rtp {disable | enable}
      set open-register-pinhole {disable | enable}
      set open-contact-pinhole {disable | enable}
      set strict-register {disable | enable}
      set register-rate <rate_sec_policy_int>
      set invite-rate <rate_sec_policy_int>
      set max-dialogs <max_int>
      set max-line-length <length_int>
      set block-long-lines {disable | enable}
      set block-unknown {disable | enable}
      set call-keepalive <keepalive_time>
      set block-ack {disable | enable}
      set block-bye {disable | enable}
      set block-cancel {disable | enable}
      set block-info {disable | enable}
      set block-invite {disable | enable}
      set block-message {disable | enable}
      set block-notify {disable | enable}
      set block-options {disable | enable}
      set block-prack {disable | enable}
      set block-publish {disable | enable}
      set block-refer {disable | enable}
      set block-register {disable | enable}
      set block-subscribe {disable | enable}
      set block-update {disable | enable}
      set reg-diff-port {disable | enable}
      set rfc2543-branch {disable | enable}
      set log-violations {disable | enable}
      set log-call-summary {disable | enable}
      set nat-trace {disable | enable}
      set subscribe-rate <rate_sec_policy_int>
      set message-rate <rate_sec_policy_int>
      set notify-rate <rate_sec_policy_int>
      set refer-rate <rate_sec_policy_int>
      set update-rate <rate_sec_policy_int>
      set options-rate <rate_sec_policy_int>
      set ack-rate <rate_sec_policy_int>
      set prack-rate <rate_sec_policy_int>
      set info-rate <rate_sec_policy_int>
      set publish-rate <rate_sec_policy_int>
      set bye-rate <rate_sec_policy_int>
      set cancel-rate <rate_sec_policy_int>
      set preserve-override {disable | enable}
      set no-sdp-fixup {disable | enable}
      set contact-fixup {disable | enable}
      set max-idle-dialogs <dialogs_perpolicy_int>
      set block-geo-red-options {disable | enable}
      set hosted-nat-traversal {disable | enable}
      set hnt-restrict-source-ip {disable | enable}
      set max-body-length <size_bytes_int>
      set unknown-header {discard | pass | respond}
      set malformed-request-line {discard | pass | respond}
      set malformed-header-via {discard | pass | respond}
      set malformed-header-from {discard | pass | respond}
      set malformed-header-to {discard | pass | respond}
      set malformed-header-call-id {discard | pass | respond}
      set malformed-header-cseq {discard | pass | respond}
      set malformed-header-rack {discard | pass | respond}
      set malformed-header-rseq {discard | pass | respond}
      set malformed-header-contact {discard | pass | respond}
      set malformed-header-record-route {discard | pass | respond}
      set malformed-header-route {discard | pass | respond}
      set malformed-header-expires {discard | pass | respond}
      set malformed-header-content-type {discard | pass | respond}
      set malformed-header-content-length {discard | pass | respond}
      set malformed-header-max-forwards {discard | pass | respond}
      set malformed-header-allow {discard | pass | respond}
      set malformed-header-p-asserted-identity {discard | pass | respond}
      set malformed-header-sdp-v {discard | pass | respond}
      set malformed-header-sdp-o {discard | pass | respond}
      set malformed-header-sdp-s {discard | pass | respond}
      set malformed-header-sdp-i {discard | pass | respond}
      set malformed-header-sdp-c {discard | pass | respond}
      set malformed-header-sdp-b {discard | pass | respond}
      set malformed-header-sdp-z {discard | pass | respond}
      set malformed-header-sdp-k {discard | pass | respond}
      set malformed-header-sdp-a {discard | pass | respond}
      set malformed-header-sdp-t {discard | pass | respond}
      set malformed-header-sdp-m {discard | pass | respond}
      set provisional-invite-expiry-time <time_int>
    config sccp
      set status {disable | enable}
      set block-mcast {enable | disable}
      set verify-header {enable | disable}
      set log-call-summary {disable | enable}
      set log-violations {disable | enable}
      set max-calls <calls_int>
  end
```

Variable	Description	Default
`edit <profile_name>`	Enter the name of a VoIP profile	
`comment <comment_str>`	Optionally enter a description of up to 63 characters of the VoIP profile.	

config sip

Configure VoIP profile settings for SIP and SIMPLE.

Variable	Description	Default
`status {disable | enable}`	Enable or disable SIP for this VoIP profile.	`enable`
`rtp {disable | enable}`	Enable or disable opening pinholes for RTP traffic to traverse FortiGate unit.	`enable`
`open-register-pinhole {disable | enable}`	Enable or disable opening a pinhole for the port number specified in SIP REGISTER message Contact header line.	`enable`
`open-contact-pinhole {disable | enable}`	Enable or disable opening a pinhole for the port number specified in a Contact header line in any SIP message except a SIP REGISTER message.	`enable`
`strict-register {disable | enable}`	Controls how pinholes are opened to allow traffic from a SIP server to pass through the FortiGate unit. If enabled the SIP ALG opens a pinhole that only accepts sessions from a single IP address (the address of the SIP server). This option should be disabled if the SIP proxy server and SIP registrar are different entities with different IP addresses.	`disable`
`register-rate <rate_sec_policy_int>`	Set a rate limit (per second, per policy) for SIP REGISTER requests. Set to 0 to disable rate limiting.	`0`
`invite-rate <rate_sec_policy_int>`	Set a rate limit (per second, per policy) for SIP INVITE requests. Set to 0 to disable rate limiting.	`0`
`max-dialogs <max_int>`	Maximum number of concurrent calls (or dialogs) per policy. Set to 0 to not limit dialogs.	`0`
`max-line-length <length_int>`	Maximum SIP header line length. The range is 78-4096 characters. If a SIP message contains a line that exceeds the maximum line length a log message is recorded. If `block-long-lines` is enabled the message is blocked and the FortiGate unit returns a SIP 413 Request entity too large SIP response message.	`998`
`block-long-lines {disable | enable}`	Enable or disable blocking SIP request messages with a header or body line that exceeds the `max-line-length`.	`enable`
`block-unknown {disable | enable}`	Block unrecognized SIP request messages.	`enable`
`call-keepalive <keepalive_time>`	Continue tracking calls with no RTP sessions for this many minutes. Terminate the call if the time limit is exceeded. Range is 1 and 10,080 seconds. Set to 0 to disable. Call keep alive should be used with caution because enabling this feature results in extra FortiGate CPU overhead and can cause delay/jitter for the VoIP call. Also, the FortiGate unit terminates the call without sending SIP messages to end the call. And if the SIP endpoints send SIP messages to terminate the call they will be blocked by the FortiGate unit if they are sent after the FortiGate unit terminates the call.	`0`
`block-ack {disable | enable}`	Enable or disable blocking SIP ACK request messages.	`disable`
`block-bye {disable | enable}`	Enable or disable blocking SIP BYE request messages.	`disable`
`block-cancel {disable | enable}`	Enable or disable blocking SIP CANCEL request messages.	`disable`

Variable	Description	Default
`block-info {disable | enable}`	Enable or disable blocking SIP INFO request messages.	`disable`
`block-invite {disable | enable}`	Enable or disable blocking SIP INVITE request messages.	`disable`
`block-message {disable | enable}`	Enable or disable blocking SIP MESSAGE request messages.	`disable`
`block-notify {disable | enable}`	Enable or disable blocking SIP NOTIFY request messages.	`disable`
`block-options {disable | enable}`	Enable or disable blocking SIP OPTIONS request messages.	`disable`
`block-prack {disable | enable}`	Enable or disable blocking SIP PRACK request messages.	`disable`
`block-publish {disable | enable}`	Enable or disable blocking SIP PUBLISH request messages.	`disable`
`block-refer {disable | enable}`	Enable or disable blocking SIP REFER request messages.	`disable`
`block-register {disable | enable}`	Enable or disable blocking SIP REGISTER request messages.	`disable`
`block-subscribe {disable | enable}`	Enable or disable blocking SIP SUBSCRIBE request messages.	`disable`
`block-update {disable | enable}`	Enable or disable blocking SIP UPDATE request messages.	`disable`
`reg-diff-port {disable | enable}`	Enable or disable opening a pinhole for the port number included in the Via SIP message header line.	`disable`
`rfc2543-branch {disable | enable}`	Enable to support RFC 2543-complaint SIP calls involving branch commands that are missing or that are valid for RFC 2543 but invalid for RFC 3261. RFC 3261 is the most recent SIP RFC. RFC 3261 obsoletes RFC 2543. This option also allows FortiGate units to support SIP calls that include Via headers that are missing the branch parameter.	`disable`
`log-violations {disable | enable}`	Enable or disable writing a logging message when a SIP option in a VoIP profile detects a violation in a SIP message.	`disable`
`log-call-summary {disable | enable}`	Enable or disable summary content archiving of SIP calls.	`enable`
`nat-trace {disable | enable}`	Enable or disable preserving the original source IP address of the SIP message in the i= line of the SDP profile. This option enables NAT with IP address conservation (also called SIP NAT tracing), which changes the contents of SIP messages by adding the source IP address of the originator of the message into the SDP i= line of the SIP message. The SDP i= line is used for free-form text. However, if your SIP server can retrieve information from the SDP i= line, it can be useful for keeping a record of the source IP address of the originator of a SIP message when operating in a NAT environment. You can use this feature for billing purposes by extracting the IP address of the originator of the message.	`enable`
`subscribe-rate <rate_sec_policy_int>`	Limit the number of SIP SUBSCRIBE messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	`0`
`message-rate <rate_sec_policy_int>`	Limit the number of SIP MESSAGE messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	`0`
`notify-rate <rate_sec_policy_int>`	Limit the number of SIP NOTIFY messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	`0`

Variable	Description	Default
refer-rate <rate_sec_policy_int>	Limit the number of SIP REFER messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
update-rate <rate_sec_policy_int>	Limit the number of SIP UPDATE messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
options-rate <rate_sec_policy_int>	Limit the number of SIP OPTIONS messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
ack-rate <rate_sec_policy_int>	Limit the number of SIP ACK messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
prack-rate <rate_sec_policy_int>	Limit the number of SIP PRACK messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
info-rate <rate_sec_policy_int>	Limit the number of SIP INFO messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
publish-rate <rate_sec_policy_int>	Limit the number of SIP PUBLISH messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
bye-rate <rate_sec_policy_int>	Limit the number of SIP BYE messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
cancel-rate <rate_sec_policy_int>	Limit the number of SIP CANCEL messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting.	0
preserve-override {disable | enable}	Enable or disable adding the original o= line of a SIP message to the end of the i= line or replace the i= line in the original message with a new i= line. This command is used for SIP IP address conservation.	disable
no-sdp-fixup {disable | enable}	Enable or disable not performing NAT on addresses in the SDP lines of the SIP message body. This option is disabled by default and the FortiGate unit performs NAT on addresses in SDP lines. Enable this option if you don’t want the FortiGate unit to perform NAT on the addresses in SDP lines.	disable
contact-fixup {disable | enable}	Enable or disable performing NAT on the IP addresses and port numbers in the headers in SIP CONTACT messages even if they don’t match the session’s IP address and port numbers.	enable
max-idle-dialogs <dialogs_perpolicy_int>	Specify the maximum number of established but idle dialogs to retain (per policy). Set to 0 to disable. Idle dialogs would usually be dialogs that have been interrupted because of errors or problems or as the result of a SIP attack that opens a large number of SIP dialogs without closing them. This command provides a way to remove these dialogs from the dialog table and recover memory and resources being used by these open and idle dialogs.	0
block-geo-red-options {disable | enable}	Block OPTIONS requests, but OPTIONS requests still notify for redundancy.	disable
hosted-nat-traversal {disable | enable}	Enable or disable support for hosted NAT Traversal (HNT). HNT has different requirements for address translation.	disable
hnt-restrict-source-ip {disable | enable}	Restrict RTP source IP to be the same as SIP source IP when HNT is enabled.	disable

Variable	Description	Default
`max-body-length <size_bytes_int>`	Specify the maximum size of a SIP message body in bytes that will be processed by the SIP ALG. Larger messages are discarded. Set to 0 for no limit. This option checks the value in the SIP Content-Length header line to determine body length. The Content-Length can be larger than the actual size of a SIP message if the SIP message content is split over more than one packet. SIP messages are of variable size and the message size can change with the addition of Via and Record-Route headers.	`0`
`unknown-header {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message with an unknown header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-request-line {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed request-line (the first line in a SIP request message). Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-via {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Via header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-from {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed From header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-to {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed To header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-call-id {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Call ID header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-cseq {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed CSeq header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-rack {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Rack header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-rseq {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed RSeq header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-contact {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Contact header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`

Variable	Description	Default
`malformed-header-record-route {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Record-Route header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-route {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Route header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-expires {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Expires header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-content-type {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Content-Type header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-content-length {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Content-Length header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-max-forwards {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Max-forwards header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-allow {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Allow header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-p-asserted-identity {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed P-Asserted-Identity header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-v {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed v= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-o {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed o= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-s {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed s= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-i {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed i= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`

Variable	Description	Default
`malformed-header-sdp-c {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed c= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-b {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed b= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-z {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed z= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-k {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed k= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-a {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed a= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-t {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed t= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-r {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed r= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`malformed-header-sdp-m {discard | pass | respond}`	Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed m= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and `log-violations` is enabled.	`pass`
`provisional-invite-expiry-time <time_int>`	The expiry time in seconds to wait for provisional INVITE requests. The range is 10-3600 seconds.	`210`

config sccp

Configure VoIP profile settings for SCCP.

Variable	Description	Default
`status {disable | enable}`	Enable or disable SCCP.	`enable`
`block-mcast {enable | disable}`	Enable or disable blocking multicast RTP connections.	`disable`
`verify-header {enable | disable}`	Enable or disable verifying SCCP header content.	`disable`
`log-call-summary {disable | enable}`	Enable or disable summary content archiving of SCCP calls.	`enable`

Variable	Description	Default
`log-violations {disable | enable}`	Enable or disable writing a logging message when a SIP option in a VoIP profile detects a violation in a SIP message.	`disable`
`max-calls <calls_int>`	Enter the maximum number of calls per minute per SCCP client. The range is 1 to 65535. Set to 0 to disable limiting the number of calls.	`0`

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.

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	Default
`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.	Fortinet-Firmware
`scep-url <scep_url>`	URL of the SCEP server used for automatic CRL certificate updates. The URL must begin with `http://` or `https://`.	
`update-vdom <update_vdom>`	VDOM used to communicate with remote SCEP server for CRL auto-update.	root

Variable	Description	Default
`http-url <http_url>`	URL of an http server used for automatic CRL certificate updates. The URL must begin with `http://` or `https://`.	
`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. This option is available when you add a `scep-url`.	

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`

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`.

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.

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

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`

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 381). 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 381).	`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`

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 381).	`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`

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 localid-type {auto | fqdn | user-fqdn | keyid | address | asn1dn}
    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 381.	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 687 and "vpn certificate ca" on page 508.	`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 486, "user ldap" on page 487, "user local" on page 489, and "user radius" on page 493.	`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 296.	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 381) 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 381).	`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.`
`localid-type {auto | fqdn | user-fqdn | keyid | address | asn1dn}`	Select the type of `localid`: `auto` — select type automatically `fqdn` — Fully Qualified Domain Name `user-fqdn` — Use User Fully Qualified Domain Name `keyid` — Use Key Identifier ID `address` — Use IP address ID `asn1dn` — Use ASN.1 Distinguished Name ID	`auto`
`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`

Variable	Description	Default
`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 490.	`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 492.	`Null.`

Variable	Description	Default
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
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>`	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 687.	`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 486, "user ldap" on page 487, "user local" on page 489, and "user radius" on page 493.	`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`

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 542)
- 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 localid-type {auto | fqdn | user-fqdn | keyid | address | asn1dn}
        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 381.	disable
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 687 and "vpn certificate ca" on page 508.	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

Variable	Description	Default
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 486, "user ldap" on page 487, "user local" on page 489, and "user radius" on page 493.	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
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 296.	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

Variable	Description	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 381) 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 ::
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 381).	0.0.0.0 for IPv4 :: for IPv6

Variable	Description	Default
`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.`
`localid-type {auto | fqdn | user-fqdn | keyid | address | asn1dn}`	Select the type of `localid`: `auto` — select type automatically `fqdn` — Fully Qualified Domain Name `user-fqdn` — Use User Fully Qualified Domain Name `keyid` — Use Key Identifier ID `address` — Use IP address ID `asn1dn` — Use ASN.1 Distinguished Name ID	`auto`
`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`
`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.	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 490.	`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.`

Variable	Description	Default
`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 492.	`Null.`
`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 687.	`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 486, “user ldap” on page 487, “user local” on page 489, and “user radius” on page 493.	`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.

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 encapsulation {tunnel-mode | transport-mode}
    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 346. For information about FortiGate DHCP relay, see “system interface” on page 381. 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`
`encapsulation {tunnel-mode | transport-mode}`	Select encapsulation: **tunnel-mode** — Encrypt both payload data and headers. **transport-mode** — Encrypt only the payload data. This is used when combining IPsec with another encapsulation, such as L2TP.	`tunnel-mode`
`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 29.	`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

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 encapsulation {tunnel-mode | transport-mode}
    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 346. For information about FortiGate DHCP relay, see "system interface" on page 381. 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
encapsulation {tunnel-mode | transport-mode}	Select encapsulation: **tunnel-mode** — Encrypt both payload data and headers. **transport-mode** — Encrypt only the payload data. This is used when combining IPsec with another encapsulation, such as GRE.	tunnel-mode
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

Variable	Description	Default
`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.

`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 29.	`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`

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 486, “user ldap” on page 487, “user local” on page 489, and “user radius” on page 493.

You need to define a firewall policy to control services inside the L2TP tunnel. For more information, see “firewall” on page 67. 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 486, “user ldap” on page 487, “user local” on page 489, and “user radius” on page 493.	`Null.`

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 486, “user ldap” on page 487, “user local” on page 489, “user radius” on page 493, “user peer” on page 490, and “user peergrp” on page 492.

You need to define a firewall policy to control services inside the PPTP tunnel. For more information, see “firewall” on page 67. 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 486, "user ldap" on page 487, "user local" on page 489, "user radius" on page 493, "user peer" on page 490, and "user peergrp" on page 492	`Null.`

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...pooln_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`

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-xxxxxxxxxxx, 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.

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 exclusive-routing {enable | disable}
        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.
`exclusive-routing {enable | disable}`	Enabling exclusive-routing adds options to allow client traffic flow control.	`disable`
`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.

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.

wanopt

Use these commands to configure FortiGate WAN optimization.

- auth-group
- peer
- rule
- settings
- ssl-server
- storage
- webcache

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 511.	
`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.	

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

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 569. 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`.	`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`

settings

Use this command to add or change the FortiGate WAN optimization local host ID and to enable traffic logging 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.	

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 511. 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

storage

Use this 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.

Syntax

```
config wanopt storage
  edit <storage_name_str>
    set size <partition_size_int>
  end
```

Variable	Description	Default
edit <storage_name_str>	Enter the name of a storage configured using the config system storage command. All FortiGate units with hard disks include a default storage name such as Internal or ASM.	
size <partition_size_int>	The size of the partition in Mbytes. The default depends on the partition size.	

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-exemtion {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}
    config cache-exemption-list
      edit <url-id_int>
        set url-pattern <url-str>
      end
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-exemtion {disable | enable}`	Enable to set a cache exemption list. User defined URLs in the list will be exempted from caching.	disable
`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

Variable	Description	Default
`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
`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

config cache-exemption-list

Configure a cache exemption list. The URLs that are defined in this list will be exempted from caching. The `url-pattern` can be an internal ip address such as “192.168.1.121” or a web address such as “example.com/test123/321” or a numeric ip address such as “1.1.1.1”.

Variable	Description	Default
`<url-id_int>`	A unique number to identify each URL entry in the list.	
`url-pattern <url-str>`	The URL added to the list.	

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 status {disable | enable}
  set ftp-over-http {disable | enable}
  set socks {disable | enable}
  set http-incoming-port <http_port_int>
  set https-incoming-port <https_port_int>
  set ftp-incoming-port <ftp_port_int>
  set socks-incoming-port <socks_port_int>
  set incoming-ip <incoming_interface_ipv4>
  set outgoing-ip <outgoing_interface_ipv4>
  set unknown-http-version {best-effort | reject}
  set realm <realm_str>
  set sec-default-action {accept | deny}
  set pac-file-server-status {disable | enable}
  set pac-file-server-port <pac_port_int>
  set pac-file-name <pac_file_str>
  set pac-file-data <pac_file_str>
  set pac-file-url <url_str>
end
```

Variable	Description	Default
`status {disable | enable}`	Enable the explicit web proxy for HTTP and HTTPS sessions.	`disable`
`ftp-over-http {disable | enable}`	Configure the explicit proxy to proxy FTP sessions sent from a web browser. The explicit proxy only supports FTP with a web browser and not with a standalone FTP client.	`disable`
`socks {disable | enable}`	Configure the explicit proxy to proxy SOCKS sessions sent from a web browser. For information about SOCKS, see RFC 1928. The explicit web proxy supports SOCKs 4 and 5.	`disable`
`http-incoming-port <http_port_int>`	Enter the port number that HTTP traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's HTTP proxy settings to use this port.	`8080`
`https-incoming-port <https_port_int>`	Enter the port number that HTTPS traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's HTTPS proxy settings to use this port. The default value of 0 means use the same port as HTTP.	`0`
`ftp-incoming-port <ftp_port_int>`	Enter the port number that FTP traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's FTP proxy settings to use this port. The default value of 0 means use the same port as HTTP.	`0`
`socks-incoming-port <socks_port_int>`	Enter the port number that SOCKS traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's SOCKS proxy settings to use this port. The default value of 0 means use the same port as HTTP.	`0`

Variable	Description	Default
`incoming-ip <incoming_interface_ipv4>`	Enter the IP address of a FortiGate unit interface that should accept sessions for the explicit web proxy. Use this command to restrict the explicit web proxy to only accepting sessions from one FortiGate interface. The destination IP address of explicit web proxy sessions should match this IP address.	`0.0.0.0`
`outgoing-ip <outgoing_interface_ipv4>`	Enter the IP address of a FortiGate unit interface that explicit web proxy sessions should exit the FortiGate unit from. Use this command to restrict the explicit web proxy to only allowing sessions to exit from one FortiGate interface. This IP address becomes the source address of web proxy sessions exiting the FortiGate unit.	`0.0.0.0`
`unknown-http-version {best-effort | reject}`	Select the action to take when the proxy server must handle an unknown HTTP version request or message. Choose from either Reject or Best Effort. Best Effort attempts to handle the HTTP traffic as best as it can. Reject treats unknown HTTP traffic as malformed and drops it. The Reject option is more secure.	`reject`
`realm <realm_str>`	Enter an authentication realm to identify the explicit web proxy. The realm can be any text string of up to 63 characters. If the realm includes spaces enclose it in quotes. When a user authenticates with the explicit proxy the HTTP authentication dialog includes the realm so you can use the realm to identify the explicit web proxy for your users.	`default`
`sec-default-action {accept | deny}`	Configure the explicit web proxy to block (deny) or accept sessions if firewall policies have note been added for the explicit web proxy. To add firewall policies for the explicit web proxy add a firewall policy and set the source interface to web-proxy. The default setting denies access to the explicit web proxy before adding a firewall policy. If you set this option to `accept` the explicit web proxy server accepts sessions even if you haven't defined a firewall policy.	`deny`
`pac-file-server-status {disable | enable}`	Enable support for proxy auto-config (PAC). With PAC support enabled you can configure a PAC file on the FortiGate unit and distribute the URL of this file to your web browser users. These users can enter this URL as an automatic proxy configuration URL and their browsers will automatically download proxy configuration settings. You can use PAC to provide access to multiple proxy servers and access methods as well as other features. To enable PAC you must edit or replace (by importing) the default PAC file installed in your FortiGate unit.	`disable`
`pac-file-server-port <pac_port_int>`	Select the port that PAC traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's PAC proxy settings to use this port. The default value of 0 means use the same port as HTTP.	`0`
`pac-file-name <pac_file_str>`	Change the name of the PAC file. In most cases you could keep the default name.	`proxy.pac`

Variable	Description	Default
`pac-file-data <pac_file_str>`	Enter the contents of the PAC file made available from the explicit proxy server for PAC support. Enclose the PAC file text in quotes. You can also copy the contents of a PAC text file and paste the contents into the CLI using this option. Enter the command followed by two sets of quotes then place the cursor between the quotes and paste the file content. The maximum PAC file size is 8192 bytes. You can use any PAC file syntax that is supported by your users's browsers. The FortiGate unit does not parse the PAC file.	

`pac-file-url <url_str>`	Displays the PAC file URL in the format:
	`http://<interface_ip>:<PAC_port_int>/<pac_file_str>`
	For example, if the interface with the explicit web proxy has IP address 172.20.120.122, the PAC port is the same as the default HTTP explicit proxy port (8080) and the PAC file name is proxy.pac the PAC file URL would be:
	`http://172.20.120.122:8080/proxy.pac`
	If the explicit web proxy is enabled on multiple interfaces there will be multiple PAC URLs. If you have configured an `incoming-ip` only one PAC file URL is listed that includes the `incoming-ip`.
	Distribute this URL to PAC users.
	You cannot use the `pac-file-url` option to edit the PAC file URL.	

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 proxy-fqdn <fqdn>
  set max-request-length <kBytes>
  set max-message-length <kBytes>
  set add-header-client-ip {disable | enable}
  set add-header-via {disable | enable}
  set add-header-x-forwarded-for {disable | enable}
  set add-header-front-end-https {disable | enable}
  set strict-web-check {disable | enable}
end
```

Variable	Description	Default
`proxy-fqdn <fqdn>`	Set the fully qualified domain name (FQDN) for the proxy. This is the domain that clients connect to.	`default.fqdn`
`max-request-length <kBytes>`	Set the maximum length, in kBytes, of the HTTP request line. Range 2 to 64.	4
`max-message-length <kBytes>`	Set the maximum length, in kBytes, of the HTTP message not including body. Range 16 to 256.	32
`add-header-client-ip {disable | enable}`	Enable to add the client IP to the header of 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`
`add-header-front-end-https {disable | enable}`	Enable to add a front-end-https header to forwarded requests.	`disable`
`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`
`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`

webfilter

Use webfilter commands to add banned words to the banned word list, filter URLs, and configure FortiGuard-Web category filtering.

This chapter contains the following sections:

content

Control web content by blocking or exempting words, phrases, or patterns.

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 48.

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.	
`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 web filter profile. `Exempt` If the pattern matches, the web page will not be blocked even if there are matching Block entries.	`block`

Variable	Description	Default
`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 web filter profile, the page is processed according to whether the `bannedword` option is set with the `http` command in the web filter 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`

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`

cookie-ovrd

Use this command to configure FortiOS Carrier browser cookie-based FortiGuard Web Filtering overrides.

Using browser cookie-based FortiGuard Web Filtering overrides you can identify users according to their web browser cookie instead of their IP address and then to use this identification to apply FortiGuard Web Filtering overrides to individual users.

Use the config user group command to configure browser cookie-based override settings in a user group. See "user group" on page 486.

Syntax

```
config webfilter cookie-ovrd
  set auth-epoch <epoch_int>
  set cookie-name <name_str>
  set redir-host <host_str>
  set redir-port <port_int>
end
```

Variable	Description	Default
`auth-epoch <epoch_int>`	Enter an integer to change the `auth-epoch` that is used to generate encrypted cookie values. Changing the auth-epoch invalidates all previous browser cookie-based overrides.	0
`cookie-name <name_str>`	The cookie that is set is `<name_str>=<encrypted override data>`. In most cases you do not need to change the default value.	
`redir-host <host_str>`	Enter a the override validation hostname to be used in cookies sent by the FortiOS Carrier unit to remote sites to support browser cookie-based overrides. Requests to this host name using the `redir-port` are permanently intercepted by the FortiOS Carrier unit. The host name can be a domain name (`example.com` or `www.example.com`) or a numeric IP address.	
`redir-port <port_int>`	Enter the override validation port number on which the FortiOS Carrier unit intercepts all requests from the `redir-host`.	20080

fortiguard

Use this command to enable Web filtering by specific categories using FortiGuard-Web URL filtering.

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 ovrd-auth-hostname <string>
  set ovrd-auth-cert <string>
  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 “prefix-list, prefix-list6” on page 273.	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`
`ovrd-auth-hostname <string>`	Enter a host name to use for FortiGuard Web Filter HTTPS override authentication.	
`ovrd-auth-cert <string>`	Enter a certificate name to use for FortiGuard Web Filter HTTPS override authentication.	`Fortinet_Firmware`
`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`

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 web filter 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`

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`

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.	

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.	

profile

Use this command to configure UTM web filtering profiles for firewall policies. Web filtering profiles configure how web filtering and FortiGuard Web Filtering is applied to sessions accepted by a firewall policy that includes the web filter profile.

Syntax

```
config webfilter profile
  edit <name_str>
    set comment <comment_str>
    set web-content-log {disable | enable}
    set web-filter-activex {disable | enable}
    set web-filter-cookie-log {disable | enable}
    set web-filter-applet-log {disable | enable}
    set web-url-log {disable | enable}
    set web-invalid-domain-log {disable | enable}
    set web-ftgd-err-log {disable | enable}
    set web-ftgd-quota-usage {disable | enable}
      config config {http | https}
        set options {activexfilter | bannedword | block-invalid-url | |
            block-ssl-unknown-sess-id | contenttype-check | cookiefilter |
            fortiguard-wf | javafilter | rangeblock | urlfilter}
        set post-action {normal | comfort | block}
      config web
        set bword-threshold <threshold_int>
        set bword-table <filter_list_name>
        set urlfilter-table <url_list_name>
        set content-header-list <list_number>
        set safe-search {bing | google | yahoo}
      config ftgd-wf
        set {http-options | https-options} {allow-ovrd | connect-request-
            bypass | error-allow | http-err-detail| rate-image-urls |
            rate-server-ip | redir-block | strict-blocking}
        set enable {all | <category_str>}
        set disable {all | <category_str>}
        set allow {all | <category_str>}
        set deny {all | <category_str>}
        set log {all | <category_str>}
        set ovrd {all | <category_str>}
        set ftgd-wf-ssl-exempt {all | <category_str>}
        set ovrd-type {dir | domain | rating | ask}
        set ovrd-cookie {allow | deny}
        set ovrd-scope {ask | ip | profile | user | user-group}
        set ovrd-ext {allow | ask | deny}
        set ovrd-dur-mode {ask | constant}
        set ovrd-dur <###d##h##m>
        set ovrd-user-group <groupname_str> [<groupname_str>...]
      config ftgd-quota
        edit <category_str>
          set quota <###d##h##m>
          set status {disable | enable | exempt}
      config url-extraction
        set status {disable | enable}
```

```
            set server-fqdn <fqdn_str>
            set redirect-header <header_str>
            set redirect-url <url_str>
            set redirect-no-content {disable | enable}
        end
    end
```

Variable	Description	Default
`<name_str>`	Enter the name of the web filtering profile.	
`comment <comment_str>`	Optionally enter a description of up to 63 characters of the web filter profile.	
`web-content-log {disable | enable}`	Enable or disable logging for web content blocking.	`disable`
`web-filter-activex {disable | enable}`	Enable or disable logging for activex script web filtering.	`disable`
`web-filter-cookie-log {disable | enable}`	Enable or disable logging for cookie script web filtering.	`disable`
`web-filter-applet-log {disable | enable}`	Enable or disable logging for applet script web filtering.	`disable`
`web-url-log {disable | enable}`	Enable or disable logging for web URL filtering.	`disable`
`web-invalid-domain-log {disable | enable}`	Enable or disable logging for web filtering of invalid domain names.	`disable`
`web-ftgd-err-log {disable | enable}`	Enable or disable logging for FortiGuard Web Filtering rating errors.	`disable`
`web-ftgd-quota-usage {disable | enable}`	Enable or disable logging for FortiGuard Web Filtering daily quota usage.	`disable`

config {http | https}

Configure HTTP or HTTPS web filtering options.

Variable	Description	Default
`options {activexfilter | bannedword | block-invalid-url | | block-ssl-unknown-sess-id | contenttype-check | cookiefilter | fortiguard-wf | javafilter | rangeblock | urlfilter}`	Select one or more options apply to http web filtering. To select more than one, enter the option names separated by a space. Some options are only available for some protocols. `activexfilter` block ActiveX plugins. `bannedword` filter based on web page content (enable web content filtering). Use `config web` to select a web content filter list and set the web content filtering threshold. `block-invalid-url` block web pages with an invalid domain name. `block-ssl-unknown-sess-id` (`https` only) 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. `contenttype-check` filter based on the content-type header. `cookiefilter` block cookies. `fortiguard-wf` enable FortiGuard Web Filtering. `javafilter` block Java applets. `rangeblock` block downloading parts of a file that have already been partially downloaded. Selecting 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. `urlfilter` filter based on URLs (enable URL filtering). Use `config web` to select a 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.	
`post-action {normal | comfort | block}`	Select the action to take with HTTP POST traffic. This option is available for HTTPS `normal` do not affect HTTP POST traffic. `comfort` use the `comfort-interval` and `comfort-amount` http options of the“firewall profile-protocol-options” on page 115 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`

config web

Specify the web content filtering the web URL filtering lists to use with the web filtering profile and set other configuration setting such as the web content filter threshold.

Variable	Description	Default
`bword-threshold <threshold_int>`	If the combined scores of the web content filter patterns appearing in a web page exceed the threshold value, the web page is blocked. The rang is 0-2147483647.	`10`
`bword-table <filter_list_name>`	Select the name of the web content filter list to use with the web filtering profile.	

Variable	Description	Default
`urlfilter-table <url_list_name>`	Select the name of the URL filter list to use with the web filtering profile.	
`content-header-list <list_number>`	Select the content header list.	`0`
`safe-search {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. 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.	

config ftgd-wf

Configure FortiGuard Web Filtering options.

For the `enable`, `disable`, `allow`, `deny`, `log`, `ovrd, ftgd-wf-ssl-exempt` options, to view a list of available category codes with their descriptions, enter `get`, then find entries 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.

Variable	Description	Default
`{http-options | https-options} {allow-ovrd | connect-request-bypass | 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. `connect-request-bypass` (`http` only) bypass FortiGuard Web Filtering for HTTP sessions to the same address as bypassed HTTPS connections. `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.	
`enable {all | <category_str>}`	Enable FortiGuard Web Filtering categories for use in local ratings. Enter `all` to enable all categories, classes, and groups or enable individual categories, classes, and groups.	all categories, classes and groups
`disable {all | <category_str>}`	Disable FortiGuard Web Filtering categories for use in local ratings. You can disable categories, classes, and groups.	
`allow {all | <category_str>}`	Enter `all`, or enter one or more category codes, representing FortiGuard Web Filtering categories or category groups that you want to allow.	all categories, classes and groups
`deny {all | <category_str>}`	Enter `all`, or enter one or more category codes, representing FortiGuard Web Filtering categories or category groups that you want to block.	
`log {all | <category_str>}`	Enter `all`, or enter one or more category codes, representing FortiGuard Web Filtering categories or category groups that you want to log.	
`ovrd {all | <category_str>}`	Enter `all`, or enter one or more category codes, representing FortiGuard Web Filtering categories or category groups that you want to allow users to override.	
`ftgd-wf-ssl-exempt {all | <category_str>}`	Enter `all`, or enter one or more category codes, representing FortiGuard Web Filtering categories or category groups that you want to exempt from SSL content inspection.	
`ovrd-type {dir | domain | rating | ask}`	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`

Variable	Description	Default
`ovrd-cookie {allow | deny}`	Allow or deny this group browser cookie-based FortiGuard Web Filtering overrides. See "webfilter cookie-ovrd" on page 585.	`deny`
`ovrd-scope {ask | ip | profile | user | user-group}`	Enter the scope of the FortiGuard Web Filtering override, one of: `ask` ask for scope when initiating an override. `ip` override for the initiating IP. `profile` override for the user's profile. `user` override for the user. `user-group` override for a user group.	`user`
`ovrd-ext {allow | ask | deny}`	Configure whether users can follow links to external sites during FortiGuard Web Filtering override: `allow` allow following links to external sites. `deny` deny following links to external sites. `ask` ask when initiating an override.	`allow`
`ovrd-dur-mode {ask | constant}`	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`
`ovrd-dur <###d##h##m>`	Enter the FortiGuard Web Filtering override duration in days, hours, and minutes in any combination. For example, `34d`, `12h`, `20m`, `34d23m`, `200d12h45m`. The maximum is 364d23h59m.	`15m`
`ovrd-user-group <groupname_str> [<groupname_str>...]`	Enter the names of user groups that can be used for FortiGuard Web Filter overrides. Separate multiple names with spaces.	

config ftgd-quota

Configure FortiGuard Web Filtering quota options for the web filtering profile to specify the length of time that users are allowed to browse each FortiGuard Web Filtering category. The timer starts when the page downloads, and stops when the user either logs out or browses to another page.

Variable	Description	Default
`edit <category_str>`	Edit a FortiGuard Web Filtering category or group to set the quota for that category or group.	
`quota <###d##h##m>`	Enter the FortiGuard Web Filtering quota duration in days, hours, and minutes in any combination. For example, `34d`, `12h`, `20m`, `34d23m`, `200d12h45m`. The maximum is 364d23h59m.	`15m`
`status {disable | enable | exempt}`	Enable or disable setting a quota for the FortiGuard Web filtering category or group. Select exempt to exempt this category or group from affecting the quota. For example, you could set a quota for a group and then exempt one or more of the categories in the group.	`disable`

config url-extraction

Configure FortiGuard Web Filtering quota options for the web filtering profile to specify the length of time that users are allowed to browse each FortiGuard Web Filtering category. The timer starts when the page downloads, and stops when the user either logs out or browses to another page.

Variable	Description	Default
`status {disable | enable}`	Edit a FortiGuard Web Filtering category or group to set the quota for that category or group.	`disable`
`server-fqdn <fqdn_str>`	Enter the full qualified domain name of the URL extraction server.	`(null)`

Variable	Description	Default
`redirect-header <header_str>`	Enter the HTTP header name to use for client redirect on blocked requests.	`x-redirect`
`redirect-url <url_str>`	Enter the HTTP header value to use for client redirect on blocked requests.	`(null)`
`redirect-no-content {disable | enable}`	Enable or disable empty message-body entity in HTTP response.	`enable`

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 | pass}
        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.	

Variable	**Description**	**Default**

`action`
`{allow | block | exempt | pass}`
	The action to take for matches.
	An `allow` match exits the URL filter list and checks the other web filters.
	A `block` match blocks the URL and no further checking will be done.
	An `exempt` match stops all further checking including AV scanning for the current HTTP session, which can affect multiple URLs.
	A `pass` match stops all further checking including AV scanning for each URL. HTML 1.1 keepalive means that sessions can include more than one URL. The `pass` action checks all URLs in a session, the `exempt` action only checks the first URL in a session and takes one action for the whole session.
		`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`

wireless-controller

Use these commands to create virtual wireless access points that can be associated with multiple physical wireless access points. Clients can roam amongst the physical access points, extending the range of the wireless network.

Note: These commands configure the wireless controller feature. They do not apply to wireless features of FortiWiFi models.

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

global

timers

vap

vap-group

wtp

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`

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`

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

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.

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.

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.

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
- batch
- carrier-license
- central-mgmt
- cfg reload
- cfg save
- clear system arp table
- cli check-template-status
- cli status-msg-only
- date
- disk
- disk raid
- dhcp lease-clear
- dhcp lease-list
- disconnect-admin-session
- enter
- factoryreset
- firmware-list update
- formatlogdisk
- fortiguard-log update
- fsae refresh
- ha disconnect
- ha manage
- ha synchronize
- interface dhcpclient-renew
- interface pppoe-reconnect
- log delete-all
- log delete-rolled
- log display
- log filter
- log fortianalyzer test-connectivity
- log list
- log recreate-sqldb
- log roll
- modem dial
- modem hangup
- modem trigger
- mrouter clear
- netscan
- npu-cli
- ping
- ping-options, ping6-options
- ping6
- reboot
- restore
- revision
- router clear bfd session
- router clear bgp
- router clear ospf process
- router restart
- send-fds-statistics
- set-next-reboot
- sfp-mode-sgmii
- shutdown
- ssh
- tac report
- telnet
- time
- traceroute
- update-ase
- update-av
- update-ips
- update-now
- upd-vd-license
- upload
- usb-disk
- vpn certificate ca
- vpn certificate crl
- vpn certificate local
- vpn certificate remote
- vpn sslvpn del-all
- vpn sslvpn del-tunnel
- vpn sslvpn del-web
- vpn sslvpn list
- wireless-controller delete-wtp-image
- wireless-controller reset-wtp
- wireless-controller restart-daemon
- wireless-controller upload-wtp-image

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 358 or “system central-management” on page 339.

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 flash <comment>
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 {ftp | tftp} <server_ipv4> netscan
```

Variable	Description
`config flash <comment>`	Back up the system configuration to the flash disk. Optionally, include a comment.
`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.

Variable	Description
`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 is 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. he disk option is 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. he disk option is 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 is available on FortiGate models that log to a hard disk.
`{disk | memory} log {ftp | tftp} <server_ipv4> netscan`	Back up the specified type of log file from either hard disk or memory to FTP or TFTP server. The disk option is 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
```

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...
```

carrier-license

bd only available on fortigate hardware running a FOC build. But disappears after you have entered a FOC license

Use this command to enter a l FortiOS Carrier license key if you are have installed a FortiOS Carrier build on a FortiGate unit and need to enter a license key to enable FortiOS Carrier functionality.

Contact Fortinet Support for more information about this command.

Syntax

```
execute carrier-license <license_key>
```

Variable	Description
`<license_key>`	Enter the FortiOS Carrier license key supplied by Fortinet.

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 339.

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
```

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.
```

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.
```

clear system arp table

Clear all the entries in the arp table.

Syntax

```
exec clear system arp table
```

cli check-template-status

Reports the status of the secure copy protocol (SCP) script template.

Syntax

```
exec cli check-template-status
```

cli status-msg-only

Enable or disable displaying standardized CLI error output messages. If executed, this command stops other debug messages from displaying in the current CLI session. This command is used for compatibility with FortiManager.

Syntax

```
exec cli status-msg-only [enable | disable]
```

Variable	Description	Default
`status-msg-only [enable | disable]`	Enable or disable standardized CLI error output messages. Entering the command without enable or disable disables displaying standardized output.	`enable`

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
```

disk

Use this command to list and format hard disks installed in FortiGate units or individual partitions on these hard disks.

Syntax

```
execute disk format <partition_ref_int>
execute disk list
```

Variable	Description
`format`	Format the referenced disk partition or disk. If you enter a partition reference number the disk partition is formatted. If you enter a disk reference number the entire disk and all of its partitions are formatted. In either case the FortiGate unit formats the partition or disk and then reboots the system. In most cases you would only need for format the entire disk if there is a problem with the partition. Formatting the partition removes all data from the partition. Formatting the disk removes all data from the entire disk and creates a single partition on the disk.
`<ref_int>`	Disk (device) or partition reference number.
`list`	List the disks and partitions including the disk partition reference number for each partition.

Examples

Use the following command to list the disks and partitions.

```
execute disk list

Device I1            29.9 GB      ref: 256        SUPER TALENT (IDE)
  partition 1        29.9 GB      ref: 257        label: 224E6EE7177E1652
```

In this example (for a FortiGate-51B), the disk (device) reference number is 256 and the reference number for the single partition is 257.

Enter the following command to format the partition.

```
execute disk format 257
```

After a confirmation message the FortiGate unit formats the partition and restarts. This can take a few minutes.

Enter the following command to format the entire disk.

```
execute disk format 256
```

After a confirmation message the FortiGate unit formats the disk, restores the original partition, and restarts. This can take a few minutes.

disk raid

Use this command to view information about and change the raid settings on FortiGate units that support RAID.

Syntax

```
execute disk raid disable
execute disk raid rebuild
execute disk raid rebuild-level {Raid-0 | Raid-1 | Raid-5}
execute disk raid status
```

Variable	Description
`disable`	Disable raid for the FortiGate unit.
`rebuild`	Rebuild RAID on the FortiGate unit at the same RAID level. You can only execute this command if a RAID error has been detected. Changing the RAID level takes a while and deletes all data on the disk array.
`rebuild-level {Raid-0 | Raid-1 | Raid-1}`	Change the RAID level on the FortiGate unit.
`status`	Display information about the RAID disk array in the FortiGate unit.

Examples

Use the following command to display information about the RAID disk array in a FortiGate-82C

```
execute disk raid status
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1000GB

Disk 1:           OK        Used     1000GB
Disk 2:           OK        Used     1000GB
Disk 3:           OK        Used     1000GB
Disk 4:  Unavailable    Not-Used        0GB
```

dhcp lease-clear

Clear all DHCP address leases.

Syntax

```
execute dhcp lease-clear
```

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.

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
```

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.

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.

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.
```

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.

fortiguard-log update

Update the FortiGuard Analysis and Management Service contract.

Syntax

```
execute fortiguard-log update
```

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
```

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
```

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.

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
```

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
```

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>
```

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
```

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
```

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
```

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`

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`

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.
```

log recreate-sqldb

Use this command to recreate SQL log database.

Syntax

```
execute log recreate-sqldb
```

log roll

Use this command to roll all log files.

Syntax

```
execute log roll
```

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 can be used if the modem is in Standalone mode.

Syntax

```
execute modem dial
```

modem hangup

Hang up the modem.

This command can be used if the modem is in Standalone mode.

Syntax

```
execute modem hangup
```

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
```

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`.

netscan

Use this command to start and stop the network vulnerability scanner and perform related functions.

Syntax

```
execute netscan import
execute netscan list
execute netscan start {discover | scan}
execute netscan status
execute netscan stop
```

Variable	Description
`import`	Import hosts discovered on the last asset discovery scan.
`list`	List the hosts discovered on the last asset discover scan.
`start {discover	scan}`	Start configured asset discovery or vulnerability scans.
`status`	Display the status of the current network vulnerability scan.
`stop`	Stop the current network vulnerability scan.

npu-cli

Display information about the performance of an AMC security processing module such as the FortiGate-ASM-CE4, FortiGate-ADM-XE2, and FortiGate-ADM-FE8. Security processing modules are also called network processing units (NPUs). This command provides a way to communicate with the NPU module CLI.

Syntax

```
execute npu-cli <amc_device_name> <commands>
```

Variable	Description
`<amc_device_name>`	Enter the name of the security processing device that you want to display information for, in the format `/dev/<device_name>`. For example: `/dev/ce4_0` for the FortiGate-ASM-CE4 module. `/dev/xe2_0` for the FortiGate-ADM-XE4 module. `/dev/fe8_0` for the FortiGate-ADM-FE4 module.
`<commands>`	Enter a command to display information. Use the `help` command to display the complete list.

Example

This example shows how to display details about how the module is processing sessions using the syn proxy.

```
#/dev/ce4_0 showsynproxy
 Total Proxied TCP Connections:             0
 Working Proxied TCP Connections:           0
 Retired TCP Connections:                   0
   Valid TCP Connections:                   0
   Attacks, No Ack From Client:             0
   No SynAck From Server:                   0
   Rst By Server (service not supportted):  0
 Client timeout setting:                    3 Seconds
 Server timeout setting:                    3 Seconds
```

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
```

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
```

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
```

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”
```

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 flash <revision>
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 flash <revision>
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>
execute restore vcm {ftp | 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 flash <revision>`	Restore the specified revision of the system configuration from the flash disk.
`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 flash <revision>`	Restore specified firmware image from flash disk.
`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.

Variable	Description
`ips tftp <filename_str> <server_ipv4>`	Download the IPS database file from a TFTP server to the FortiGate unit.
`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. Available 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. Available 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. Available 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.
`vcm {ftp | tftp} <filename_str> <server_ipv4>`	Restore VCM engine/plugin from an ftp or tftp server.

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
```

revision

Use these commands to manage configuration and firmware image files on the local disk.

Syntax

To delete a configuration file

```
execute revision delete config <revision>
```

To delete a firmware image file

```
execute revision delete image <revision>
```

To list the configuration files

```
execute revision list config
```

To delete a firmware image file

```
execute revision list image
```

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.

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.

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
```

router restart

Use this command to restart the routing software.

Syntax

```
execute router restart
```

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
```

set-next-reboot

Use this command to start the FortiGate unit with primary or secondary firmware after the next reboot. Available on models that can 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}
```

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.

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'
```

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 #
```

tac report

Use this command to create a debug report to send to Fortinet Support. Normally you would only use this command if requested to by Fortinet Support.

Syntax

```
execute tac report
```

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.

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
```

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.

update-ase

Use this command to manually initiate the antispam engine and rules update.

Syntax

```
execute update-ase
```

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
```

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
```

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
```

upd-vd-license

Use this command to enter a Virtual Domain (VDOM) license key.

If you have a FortiGate- unit that supports VDOM licenses, 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.

Available on FortiGate models that can be licensed for more than 10 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.

upload

Use this command to upload system configurations and firmware images to the flash disk from FTP, TFTP, or USB sources.

Syntax

To upload configuration files:

```
execute upload config ftp <filename_str> <comment> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> [<password_str>]]
   [<backup_password_str>]
execute upload config tftp <filename_str> <comment> <server_ipv4>
execute upload config usb <filename_str> <comment>
```

To upload firmware image files:

```
execute upload image ftp <filename_str> <comment> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> [<password_str>]]
execute upload config tftp <filename_str> <comment> <server_ipv4>
execute upload config usb <filename_str> <comment>
```

To upload report image files:

```
execute upload report-img ftp <filename_str> <server_ipv4[:port_int] |
   server_fqdn[:port_int]> [<username_str> [<password_str>]]
execute upload report-img tftp <filename_str> <server_ipv4>
```

Variable	Description
`<comment>`	Comment string.
`<filename_str>`	Filename to upload.
`<server_fqdn[:port_int]>`	Server fully qualified domain name and optional port.
`<server_ipv4[:port_int]>`	Server IP address and optional port number.
`<username_str>`	Username required on server.
`<password_str>`	Password required on server.
`<backup_password_str>`	Password for backup file.

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.

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
```

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.

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 688 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
```

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.

vpn sslvpn del-all

Use this command to delete all SSL VPN connections in this VDOM.

Syntax

```
execute vpn sslvpn del-all
```

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.

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.

vpn sslvpn list

Use this command to list current SSL VPN tunnel connections.

Syntax

```
execute vpn sslvpn list {web | tunnel}
```

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
```

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.

wireless-controller restart-daemon

Use this command to restart the wireless-controller feature.

Syntax

```
execute wireless-controller restart-daemon
```

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>
```

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

Use this command to retrieve information about predefined application detection signatures for Endpoint NAC.

Syntax

```
get endpoint-control app-detect predefined-category status
get endpoint-control app-detect predefined-group status
get endpoint-control app-detect predefined-signature status
get endpoint-control app-detect predefined-vendor status
```

Example output (partial)

```
get endpoint-control app-detect predefined-category status
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


get endpoint-control app-detect predefined-group status
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


get endpoint-control app-detect predefined-signature status
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
```

```
get endpoint-control app-detect predefined-vendor status
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
```

firewall dnstranslation

Use this command to display the firewall DNS translation table.

Syntax

```
get firewall dnstranslation
```

firewall iprope appctrl

Use this command to list all application control signatures added to an application control list and display a summary of the application control configuration.

Syntax

```
get firewall iprope appctrl {list | status}
```

Example output

In this example, the FortiGate unit includes one application control list that blocks the FTP application.

```
get firewall iprope appctrl list
app-list=app_list_1/2000 other-action=Pass
  app-id=15896      list-id=2000  action=Block


get firewall iprope appctrl status
appctrl table 3 list 1 app 1 shaper 0
```

firewall iprope list

Use this command to list all of the FortiGate unit iprope firewall policies. Optionally include a group number in hexidecimal format to display a single policy. Policies are listed in FortiOS format.

Syntax

```
get firewall iprope list [<group_number_hex>]
```

Example output

```
get firewall iprope list 0010000c

policy flag (8000000): pol_stats
flag2 (20): ep_block shapers: / per_ip=
imflag: sockport: 1011 action: redirect index: 0
schedule() group=0010000c av=00000000 au=00000000 host=0 split=00000000
chk_client_info=0x0 app_list=0 misc=0 grp_info=0 seq=0 hash=0
npu_sensor_id=0
  tunnel=
zone(1): 0 ->zone(1): 0
source(0):
dest(0):
source wildcard(0):
destination wildcard(0):
service(1):
        [6:0x8:1011/(0,65535)->(80,80)]
nat(0):
mms: 0 0
```

firewall service predefined

Use this command to retrieve information about predefined services. If you do not specify a <service_name> the command lists all of the pre-defined services.

Syntax

```
  get firewall service predefined [<service_name>]
```

Example output

```
get firewall service predefined FTP
name                : FTP
icmpcode            :
icmptype            :
protocol            : TCP/UDP/SCTP
protocol-number     : 6
sctpport-range      :
tcpport-range       : 21:0-65535
udpport-range       :


get firewall service predefined SIP
name                : SIP
icmpcode            :
icmptype            :
protocol            : TCP/UDP/SCTP
protocol-number     : 17
sctpport-range      :
tcpport-range       :
udpport-range       : 5060:0-65535


get firewall service predefined AOL
name                : AOL
icmpcode            :
icmptype            :
protocol            : TCP/UDP/SCTP
protocol-number     : 6
sctpport-range      :
tcpport-range       : 5190-5194:0-65535
udpport-range       :
```

firewall proute

Use this command to list policy routes.

Syntax

```
get firewall proute
```

Example output

```
get firewall proute
list route policy info(vf=root):
iff=5 src=1.1.1.0/255.255.255.0 tos=0x00 tos_mask=0x00 dst=0.0.0.0/0.0.0.0
protocol=80 port=1:65535
        oif=3 gwy=1.2.3.4
```

grep

In many cases the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large get or show command output you can use the grep command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX grep, used for searching text output based on regular expressions.

Information about how to use grep and regular expressions is available from the Internet. For example, see http://www.opengroup.org/onlinepubs/009695399/utilities/grep.html.

Syntax

```
{get | show| diagnose} | grep <regular_expression>
```

Example output

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr                  00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
19:tcp     1110   10.31.101.10:1862 172.20.120.122:30670 69.111.193.57:1469
    -
27:tcp    3599  10.31.101.10:2061 -            10.31.101.100:22 -
38:tcp     3594   10.31.101.10:4780 172.20.120.122:49700 172.20.120.100:445
    -
43:tcp     3582   10.31.101.10:4398 172.20.120.122:49574
    24.200.188.171:48726 -
```

Use the following command to display all lines in HTTP replacement message commands that contain `URL` (upper or lower case):

```
show system replacemsg http | grep -i url
set buffer "<HTML><BODY>The page you requested has been blocked because it
    contains a banned word. URL = %%PROTOCOL%%%%URL%%</BODY></HTML>"
config system replacemsg http "url-block"
     set buffer "<HTML><BODY>The URL you requested has been blocked. URL =
    %%URL%%</BODY></HTML>"
config system replacemsg http "urlfilter-err"
  .
  .
  .
```

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
```

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 output

```
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"
```

hardware cpu

Use this command to display detailed information about all of the CPUs in your FortiGate unit.

Syntax

```
get hardware cpu
```

Example output

```
get hardware npu legacy list
No npu ports are found

620_ha_1 # get hardware cpu
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 15
model name      : Intel(R) Core(TM)2 Duo CPU     E4300  @ 1.80GHz
stepping        : 13
cpu MHz         : 1795.545
cache size      : 64 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 10
wp              : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe lm pni monitor ds_cpl
tm2 est
bogomips        : 3578.26

processor       : 1
vendor_id       : GenuineIntel
cpu family      : 6
model           : 15
model name      : Intel(R) Core(TM)2 Duo CPU     E4300  @ 1.80GHz
stepping        : 13
cpu MHz         : 1795.545
cache size      : 64 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 10
wp              : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe lm pni monitor ds_cpl
tm2 est
bogomips        : 3578.26
```

hardware memory

Use this command to display information about FortiGate unit memory use including the total, used, and free memory.

Syntax

```
get hardware memory
```

Example output

```
get hardware memory
        total:    used:    free:  shared: buffers:  cached: shm:
Mem:  3703943168 348913664 3355029504        0   192512 139943936 137314304
Swap:        0        0        0
MemTotal:      3617132 kB
MemFree:       3276396 kB
MemShared:           0 kB
Buffers:           188 kB
Cached:         136664 kB
SwapCached:          0 kB
Active:          22172 kB
Inactive:       114740 kB
HighTotal:     1703936 kB
HighFree:      1443712 kB
LowTotal:      1913196 kB
LowFree:       1832684 kB
SwapTotal:           0 kB
SwapFree:            0 kB
```

hardware nic

Use this command to display hardware and status information about each FortiGate interface. The hardware information includes details such as the driver name and version and chip revision. Status information includes transmitted and received packets, and different types of errors.

Syntax

```
get hardware nic <interface_name>
```

Variable	Description
`<interface_name>`	A FortiGate interface name such as port1, wan1, internal, etc.

Example output

```
get hardware nic port9
Chip_Model         FA2/ISCP1B-v3/256MB
FPGA_REV_TAG       06101916
Driver Name        iscp1a/b-DE
Driver Version     0.1
Driver Copyright   Fortinet Inc.

Link               down
Speed              N/A
Duplex             N/A
State              up

Rx_Packets         0
Tx_Packets         0
Rx_Bytes           0
Tx_Bytes           0

Current_HWaddr     00:09:0f:77:09:68
Permanent_HWaddr   00:09:0f:77:09:68

Frame_Received     0
Bad Frame Received 0
Tx Frame           0
Tx Frame Drop      0
Receive IP Error   0
FIFO Error         0

Small PktBuf Left  125
Normal PktBuf Left 1021
Jumbo PktBuf Left  253
NAT Anomaly        0
```

hardware npu

Use this command to display information about the network processor unit (NPU) hardware installed in a FortiGate unit. The NPUs can be built-in or on an installed AMC module.

Syntax

```
get hardware npu legacy {list | session <device_name_str> | setting
   <device_name_str>}
get hardware npu np1 {list | status}
get hardware npu np2 {list | performance <device_id_int> | status
   <device_id_int>}
get hardware npu np4 {list | status <device_id_int>}
```

Example output

```
get hardware npu np1 list
ID          Interface
0           port9 port10

get hardware npu np1 status
ISCP1A 10ee:0702
RX SW Done 0 MTP 0x00000000
desc_size  = 0x00001000 count    = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
Total Number of Interfaces: 2
Number of Interface In-Use: 2
Interface[0] Tx done: 0
desc_size  = 0x00004000 count    = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
TX timeout = 0x00000000 BD_empty = 0x00000000
HRx Packets= 0x00000000 HTXBytes = 0x00000000 HRXBytes = 0x00000000
Interface[1] Tx done: 0
desc_size  = 0x00004000 count    = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
TX timeout = 0x00000000 BD_empty = 0x00000000
HRx Packets= 0x00000000 HTXBytes = 0x00000000 HRXBytes = 0x00000000
NAT Information:
head       = 0x00000001 tail     = 00000001
ISCP1A Performance [Top]:
Nr_int   : 0x00000000      INTwoInd  : 0x00000000     RXwoDone  : 0x00000000
PKTwoEnd  : 0x00000000     PKTCSErr  : 0x00000000
PKTidErr : 0x00000000      PHY0Int   : 0x00000000     PHY1INT   : 0x00000000
CSUMOFF  : 0x00000000      BADCSUM   : 0x00000000     MSGINT    : 0x00000000
IPSEC    : 0x00000000      IPSVLAN   : 0x00000000     SESMISS   : 0x00000000
TOTUP    : 0x00000000      RSVD MEMU : 0x00000010
MSG Performance:
QLEN:   0x00001000(QW) HEAD: 0x00000000
Performance:
TOTMSG: 0x00000000 BADMSG: 0x00000000 TOUTMSG: 0x00000000 QUERY: 0x00000000
NULLTK: 0x00000000
NAT Performance: BYPASS (Enable) BLOCK (Disable)
IRQ    : 00000001 QFTL   : 00000000 DELF  : 00000000 FFTL  : 00000000
OVTH   : 00000001 QRYF   : 00000000 INSF  : 00000000 INVC  : 00000000
```

```
ALLO   : 00000000 FREE   : 00000000 ALLOF : 00000000 BPENTR: 00000000 BKENTR:
00000000
PBPENTR: 00000000 PBKENTR: 00000000 NOOP  : 00000000 THROT :
00000000(0x002625a0)
SWITOT : 00000000 SWDTOT : 00000000 ITDB  : 00000000 OTDB  : 00000000
SPISES : 00000000 FLUSH  : 00000000
APS (Disabled) information:
MODE: BOTH UDPTH 255 ICMPTH 255 APSFLAGS: 0x00000000
IPSEC Offload Status: 0x58077dcb
```

```
get hardware npu np2 list
ID       PORTS
--       -----
0        amc-sw1/1
0        amc-sw1/2
0        amc-sw1/3
0        amc-sw1/4
ID       PORTS
--       -----
1        amc-dw2/1
ID       PORTS
--       -----
2        amc-dw2/2
```

```
get hardware npu np2 status 0
NP2 Status

ISCP2 f7750000 (Neighbor 00000000) 1a29:0703 256MB Base f8aad000 DBG
0x00000000
RX SW Done 0 MTP 0x0
desc_alloc = f7216000
desc_size  = 0x2000 count   = 0x100
nxt_to_u   = 0x0 nxt_to_f = 0x0
Total Interfaces: 4 Total Ports: 4
Number of Interface In-Use: 4
Interface f7750100 netdev 81b1e000 0 Name amc-sw1-1
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f7750694, 00000000, 00000000, 00000000
Port f7750694 Id 0 Status Down ictr 4
desc = 8128c000
desc_size  = 0x00001000 count     = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
Intf f7750100
Interface f7750264 netdev 81b2cc00 1 Name amc-sw1-2
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f7750748, 00000000, 00000000, 00000000
Port f7750748 Id 1 Status Down ictr 0
desc = 81287000
desc_size  = 0x00001000 count     = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
Intf f7750264
Interface f77503c8 netdev 81b2c800 2 Name amc-sw1-3
```

```
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f77507fc, 00000000, 00000000, 00000000
Port f77507fc Id 2 Status Down ictr 0
desc = 81286000
desc_size  = 0x00001000 count     = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
Intf f77503c8
Interface f775052c netdev 81b2c400 3 Name amc-sw1-4
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f77508b0, 00000000, 00000000, 00000000
Port f77508b0 Id 3 Status Down ictr 0
desc = 81281000
desc_size  = 0x00001000 count     = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
Intf f775052c
NAT Information:
cmdq_qw    = 0x2000 cmdq     = 82160000
head       = 0x1 tail     = 0x1
APS (Enabled) information:
Session Install when TMM TSE OOE: Disable
Session Install when TMM TAE OOE: Disable
IPS anomaly check policy: Follow config
MSG Base = 82150000 QL = 0x1000 H = 0x0
```

hardware status

Report information about the FortiGate unit hardware including FortiASIC version, CPU type, amount of memory, flash drive size, hard disk size (if present), USB flash size (if present), network card chipset, and wifi chipset (FortiWifi models). This information can be useful for troubleshooting, providing information about your FortiGate unit to Fortinet Support, or confirming the features that your FortiGate model supports.

Syntax

```
  get hardware status
```

Example output

```
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)
```

ips decoder status

Displays all the port settings of all the IPS decoders.

Syntax

```
get ips decoder status
```

Example 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.

ips rule status

Displays current configuration information about IPS rules.

Syntax

```
get ips rule status
```

Example 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
```

ips session

Displays current IPS session status.

Syntax

```
get ips session
```

Example output

```
get ips session

SYSTEM:
memory capacity            279969792
memory used                5861008
recent pps\bps             0\0K
session in-use             0
TCP:  in-use\active\total  0\0\0
UDP:  in-use\active\total  0\0\0
ICMP: in-use\active\total  0\0\0
```

ipsec tunnel list

List the current IPSec VPN tunnels and their status.

Syntax

```
get ipsec tunnel list
```

Example output

```
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
```

Variable	Description
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.

log sql status

Display the size of the SQL reporting database.

Syntax

```
get log sql status
```

netscan settings

Use this command to display tcp and udp ports that are scanned by the current scan mode.

Syntax

```
get netscan settings
```

Example output

```
scan-mode : full
tcp-ports : 1-65535
udp-ports : 1-65535
```

report database schema

Use this command to display the FortiGate SQL reporting database schema.

Syntax

```
get report database schema
```

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
```

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 output

```
get router info bgp memory
```

```
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
```

router info isis

Use this command to display information about the FortiGate ISIS.

Syntax

```
get router info isis interface
get router info isis neighbor
get router info isis is-neighbor
get router info isis database
get router info isis route
get router info isis topology
```

router info kernel

Use this command to display the FortiGate kernel routing table. The kernel routing table displays information about all of the routes in the kernel.

Syntax

```
get router info kernel [<routing_type_int>]
```

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.

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.

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
```

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.

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.

router info vrrp

Use this command to display information about the VRRP configuration.

Syntax

```
get router info vrrp
```

Example output

```
Interface: port1, primary IP address: 9.1.1.2
  VRID: 1
    vrip: 9.1.1.254, priority: 100, state: BACKUP
    adv_interval: 1, preempt: 1, start_time: 3
    vrdst: 0.0.0.0
```

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.

router info6 interface

Use this command to display information about IPv6 interfaces.

Syntax

```
get router info6 interface <interface_name>
```

Example output

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
```

router info6 ospf

Use this command to display information about the OSPF IPv6 configuration.

Syntax

```
get router info6 ospf
```

router info6 protocols

Use this command to display information about the configuration of all IPv6 dynamic routing protocols.

Syntax

```
get router info6 protocols
```

router info6 rip

Use this command to display information about the RIPng configuration.

Syntax

```
get router info6 rip
```

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.

system admin list

View a list of all the current administration sessions.

Syntax

```
get system admin list
```

Example output

```
# 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.

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

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 output

```
# 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
```

system auto-update

Use this command to display information about the status FortiGuard updates on the FortiGate unit.

Syntax

```
get system auto-update status
get system auto-update versions
```

Example output

```
get system auto-update status
FDN availability:  available at Thu Apr  1 08:22:58 2010

Push update: disable
Scheduled update: enable
     Update daily:   8:22
Virus definitions update: enable
IPS definitions update: enable
Server override: disable
Push address override: disable
Web proxy tunneling: disable
```

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"
```

system checksum

View the checksums for global, root, and all configurations. These checksums are used by HA to compare the configurations of each cluster unit.

Syntax

```
get system checksum status
```

Example output

```
# 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
```

system cmdb status

View information about cmdbsvr on the FortiGate unit. FortiManager uses some of this information.

Syntax

```
get system cmdb status
```

Example output

```
# 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
```

Variable	Description
`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.

system dashboard

List the available dashboard widgets. The `help:` field explains widget purpose.

FortiManager uses this information.

Syntax

```
get system dashboard [<widget_name>]
```

Example output

```
# 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
```

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
```

system fortianalyzer-connectivity

Display connection and remote disk usage information about a connected FortiAnalyzer unit.

Syntax

```
get fortianalyzer-connectivity status
```

Example output

```
# get system fortianalyzer-connectivity status
Status: connected
Disk Usage: 0%
```

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 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
```

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 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
```

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.

Variable	Description
`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.

Variable	Description
`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.

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 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
```

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.

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
```

system performance firewall

Use this command to display packet distribution and traffic statistics information for the FortiGate firewall.

Syntax

```
get system performance firewall packet-distribution
get system performance firewall statistics
```

Variable	Description
`packet-distribution`	Display a list of packet size ranges and the number of packets of each size accepted by the firewall since the system restarted. You can use this information to learn about the packet size distribution on your network.
`statistics`	Display a list of traffic types (browsing, email, DNS etc) and the number of packets and number of payload bytes accepted by the firewall for each type since the FortiGate unit was restarted.

Example output

```
get system performance firewall packet-distribution
getting packet distribution statistics...
0 bytes - 63 bytes: 655283 packets
64 bytes - 127 bytes: 1678278 packets
128 bytes - 255 bytes: 58823 packets
256 bytes - 383 bytes: 70432 packets
384 bytes - 511 bytes: 1610 packets
512 bytes - 767 bytes: 3238 packets
768 bytes - 1023 bytes: 7293 packets
1024 bytes - 1279 bytes: 18865 packets
1280 bytes - 1500 bytes: 58193 packets
 > 1500 bytes: 0 packets

get system performance firewall statistics
getting traffic statistics...
Browsing: 623738 packets, 484357448 bytes
DNS: 5129187383836672 packets, 182703613804544 bytes
E-Mail: 23053606 packets, 2 bytes
FTP: 0 packets, 0 bytes
Gaming: 0 packets, 0 bytes
IM: 0 packets, 0 bytes
Newsgroups: 0 packets, 0 bytes
P2P: 0 packets, 0 bytes
Streaming: 0 packets, 0 bytes
TFTP: 654722117362778112 packets, 674223966126080 bytes
VoIP: 16834455 packets, 10 bytes
Generic TCP: 266287972352 packets, 8521215115264 bytes
Generic UDP: 0 packets, 0 bytes
Generic ICMP: 0 packets, 0 bytes
Generic IP: 0 packets, 0 bytes
```

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
```

Variable	Description
`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.

Example output

```
# 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
```

system performance top

Use this command to display the list of processes running on the FortiGate unit (similar to the Linux `top` command).

You can use the following commands when `get system performance top` is running:

- Press Q or Ctrl+C to quit.
- Press P to sort the processes by the amount of CPU that the processes are using.
- Press M to sort the processes by the amount of memory that the processes are using.

Syntax

```
get system performance top [<delay_int>] <max_lines_int>]]
```

Variable	Description
`<delay_int>`	The delay, in seconds, between updating the process list. The default is 5 seconds.
`<max_lines_int>`	The maximum number of processes displayed in the output. The default is 20 lines.

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 output

```
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    -
```

Variable	Description
`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.

system startup-error-log

Use this command to display information about system startup errors. This command only displays information if an error occurs when the FortiGate unit starts up.

Syntax

```
get system startup-error-log
```

system session status

Use this command to display 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 output

```
The total number of sessions for the current VDOM: 3100
```

system session-helper-info list

Use this command to list the FortiGate session helpers and the protocol and port number configured for each one.

Syntax

```
get system sesion-helper-info list
```

Example output

```
list builtin help module:
mgcp
dcerpc
rsh
pmap
dns-tcp
dns-udp
rtsp
pptp
sip
mms
tns
h245
h323
ras
tftp
ftp
list session help:
help=pmap, protocol=17 port=111
help=rtsp, protocol=6 port=8554
help=rtsp, protocol=6 port=554
help=pptp, protocol=6 port=1723
help=rtsp, protocol=6 port=7070
help=sip, protocol=17 port=5060
help=pmap, protocol=6 port=111
help=rsh, protocol=6 port=512
help=dns-udp, protocol=17 port=53
help=tftp, protocol=17 port=69
help=tns, protocol=6 port=1521
help=mgcp, protocol=17 port=2727
help=dcerpc, protocol=17 port=135
help=rsh, protocol=6 port=514
help=ras, protocol=17 port=1719
help=ftp, protocol=6 port=21
help=mgcp, protocol=17 port=2427
help=dcerpc, protocol=6 port=135
help=mms, protocol=6 port=1863
help=h323, protocol=6 port=1720
```

system session-info

Use this command to display session information.

Syntax

```
get system session-info expectation
get system session-info full-stat
get system session-info list
get system session-info statistics
get system session-info ttl
```

Variable	Description
`expectation`	Display expectation sessions.
`full-stat`	Display detailed information about the FortiGate session table including a session table and expect session table summary, firewall error statistics, and other information.
`list`	Display detailed information about all current FortiGate sessions. For each session the command displays the protocol number, traffic shaping information, policy information, state information, statistics and other information.
`statistics`	Display the same information as the `full-stat` command except for the session table and expect session table summary.
`ttl`	Display the current setting of the `config system session-ttl` command including the overall session timeout as well as the timeouts for specific protocols.

Example output

```
get system session-info statistics
misc info:               session_count=15 exp_count=0 clash=0
memory_tension_drop=0 ephemeral=1/32752 removeable=14
delete=0, flush=0, dev_down=0/0
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000001
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=227 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

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
- the revision of the wifi chip in a FortiWiFi unit

Syntax

```
get system status
```

Example output

```
Version: Fortigate-620B v4.0,build0271,100330 (MR2)
Virus-DB: 11.00643(2010-03-31 17:49)
Extended DB: 11.00643(2010-03-31 17:50)
Extreme DB: 0.00000(2003-01-01 00:00)
IPS-DB: 2.00778(2010-03-31 12:55)
FortiClient application signature package: 1.167(2010-04-01 10:11)
Serial-Number: FG600B3908600705
BIOS version: 04000006
Log hard disk: Available
Hostname: 620_ha_1
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Distribution: International
Branch point: 271
Release Version Information: MR2
System time: Thu Apr  1 15:27:29 2010
```

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 475.

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
```

test

Use this command to display information about FortiGate applications and perform operations on FortiGate applications. You can specify an application name and a test level. Enter ? to display the list of applications. The test level performs various functions depending on the application but can include displaying memory usage, dropping connections and restarting the application.

The test levels are different for different applications. In some cases when you enter the command and include an application name but no test level (or an invalid test level) the command output includes a list of valid test levels.

Syntax

```
get test <application_name_str> <test_level_int>
```

Example output

```
get test http
Proxy Worker 0 - http
[0:H] HTTP Proxy Test Usage
[0:H]
[0:H]     2: Drop all connections
[0:H]    22: Drop max idle connections
[0:H]   222: Drop all idle connections
[0:H]     4: Display connection stat
[0:H]    44: Display info per connection
[0:H]   444: Display connections per state
[0:H]  4444: Display per-VDOM statistics
[0:H] 44444: Display information about idle connections
[0:H]    55: Display tcp info per connection


get test http 4
HTTP Common
Current Connections                                   0/8032

HTTP Stat
Bytes sent                                            0 (kb)
Bytes received                                        0 (kb)
Error Count (alloc)                                   0
Error Count (accept)                                  0
Error Count (bind)                                    0
Error Count (connect)                                 0
Error Count (socket)                                  0
Error Count (read)                                    0
Error Count (write)                                   0
Error Count (retry)                                   0
Error Count (poll)                                    0
Error Count (scan reset)                              0
Error Count (urlfilter wait)                          0
Last Error                                            0
Web responses clean                                   0
Web responses scan errors                             0
Web responses detected                                0
Web responses infected with worms                     0
Web responses infected with viruses                   0
Web responses infected with susp                      0
Web responses file blocked                            0
Web responses file exempt                             0
Web responses bannedword detected                     0
Web requests oversize pass                            0
Web requests oversize block                           0
URL  requests exempt                                  0
URL  requests blocked                                 0
URL  requests passed                                  0
URL  requests submit error                            0
URL  requests rating error                            0
URL  requests rating block                            0
URL  requests rating allow                            0
URL  requests infected with worms                     0
Web  requests detected                                0
Web  requests file blocked                            0
Web  requests file exempt                             0
POST requests clean                                   0
POST requests scan errors                             0
POST requests infected with viruses                   0
POST requests infected with susp                      0
POST requests file blocked                            0
POST requests bannedword detected                     0
POST requests oversize pass                           0
POST requests oversize block                          0
Web request  backlog drop                             0
Web response backlog drop                             0

HTTP Accounting
setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
urlfilter=0/0/0 uf_lookupf=0
scan=0 clt=0 srv=0
```

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.

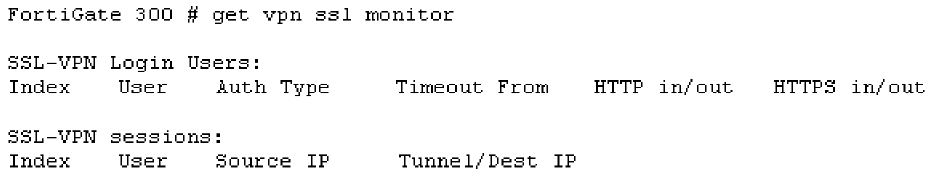
vpn ssl monitor

Use this command to display information about logged in SSL VPN users and current SSL VPN sessions.

Syntax

```
get vpn ssl monitor
```

Example 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
```

vpn status concentrators

Use this command to display information about configured IPsec VPN concentrators in a virtual domain. The command lists all the configured concentrators and for each one displays the number of tunnels in the concentrator and other information.

Syntax

```
  get vpn status ike concentrators [<arguements>]
```

Example output

```
get vpn status concentrators
list all ipsec concentrator in vd 0
name=VPN_Conc_1           ref=2          tuns=1 flags=0
```

vpn status ike

Use this command to display information the FortiGate IPsec VPN IKE configuration.

Syntax

```
get vpn status ike config
get vpn status ike crypto
get vpn status ike errors
get vpn status ike gateway [<gateway_name_str>]
get vpn status ike routes
get vpn status ike status {detailed | summary}
```

Variable	Description
`config`	List the FortiGate IPsec VPN IKE configurations, consisting of all phase 1 configurations and the associated Phase 2 configurations.
`crypto`	Display the FortiGate hardware and software crypto configuration.
`errors`	Display a list of IPsec VPN error types and the number of errors of each type that were recorded since the FortiGate unit last started.
`gateway [<gateway_name_str>]`	Display the status of one or more IPsec VPN IKE gateways. You can enter the name of the gateway to display.
`routes`	Display the status of the current IPsec VPN IKE routes.
`status`	Display the current status of all configured IPsec VPN tunnels.

Example output

```
get vpn status ike status detailed

vd: root/0
name: GateWay_1
version: 1
ISAKMP SA: created 0/0
IPsec SA: created 0/0

vd: root/0
name: GateWay_1
version: 2
ISAKMP SA: created 0/0
IPsec SA: created 0/0

vd: root/0
name: GateWay_1
version: 1
ISAKMP SA: created 0/0
IPsec SA: created 0/0
```

vpn status ipsec

Use this command to display information about all of the IPsec crypto devices available on a FortiGate unit. The out can include information about the FortiAsic and network processor ASIS, and software encryption. For each crypto device the command lists encryption and authentication algorithms and the number of each type that the crypto device is running.

Syntax

```
get vpn status ipsec
```

Example output

```
get vpn status ipsec
All ipsec crypto devices in use:
CP6:
        null:   0       0
        des:    0       0
        3des:   0       0
        aes:    0       0
        null:   0       0
        md5:    0       0
        sha1:   0       0
        sha256: 0       0
SOFTWARE:
        null:   0       0
        des:    0       0
        3des:   0       0
        aes:    0       0
        null:   0       0
        md5:    0       0
        sha1:   0       0
        sha256: 0       0
```

vpn status l2tp

Use this command to display information about L2TP tunnels.

Syntax

```
get vpn status l2tp
```

vpn status pptp

Use this command to display information about PPTP tunnels.

Syntax

```
get vpn status pptp
```

vpn status ssl

Use this command to display SSL VPN tunnels and to also verify that the FortiGate unit includes the CP6 or greater FortiASIC device that supports SSL acceleration.

Syntax

```
get vpn status ssl hw-acceleration-status
get vpn status ssl list
```

Variable	Description
`hw-acceleration-status`	Display whether or not the FortiGate unit contains a FortiASIC device that supports SSL acceleration.
`list`	Display information about all configured SSL VPN tunnels.

vpn status tunnel

Use this command to display SSL VPN tunnels and to also verify that the FortiGate unit includes the CP6 or greater FortiASIC device that supports SSL acceleration.

Syntax

```
get vpn status tunnel dialup-list <arguments>
get vpn status tunnel list
get vpn status tunnel name <tunnel_name_str>
get vpn status tunnel number <start_int> <end_int>
get vpn status tunnel stat
```

Variable	Description
`dialup-list <arguments>`	List all dialup tunnels.
`list`	List all VPN tunnels.
`name <tunnel_name_str>`	Enter the name of a tunnel to display information about it.
`number <start_int> <end_int>`	Enter a number range to list tunnels within the number range. The range can start at 0.
`stat`	Display VPN tunnel statistics.

webfilter ftgd-statistics

Use this command to display FortiGuard Web Filtering rating cache and daemon statistics.

Syntax

```
get webfilter ftgd-statistics
```

Example output

```
get webfilter ftgd-statistics

Rating Statistics:
=====================
DNS failures                     :          0
DNS lookups                      :          0
Data send failures               :          0
Data read failures               :          0
Wrong package type               :          0
Hash table miss                  :          0
Unknown server                   :          0
Incorrect CRC                    :          0
Proxy request failures           :          0
Request timeout                  :          0
Total requests                   :          0
Requests to FortiGuard servers   :          0
Server errored responses         :          0
Relayed rating                   :          0
Invalid profile                  :          0

Allowed                          :          0
Blocked                          :          0
Logged                           :          0
Errors                           :          0

Cache Statistics:
=====================
Maximum memory                   :          0
Memory usage                     :          0

Nodes                            :          0
  Leaves                         :          0
  Prefix nodes                   :          0
  Exact nodes                    :          0

Requests                         :          0
Misses                           :          0
Hits                             :          0
  Prefix hits                    :          0
  Exact hits                     :          0

No cache directives              :          0
Add after prefix                 :          0
Invalid DB put                   :          0
DB updates                       :          0
```

```
Percent full                     :          0%
  Branches                       :          0%
  Leaves                         :          0%
    Prefix nodes                 :          0%
    Exact nodes                  :          0%

Miss rate                        :          0%
Hit rate                         :          0%
  Prefix hits                    :          0%
  Exact hits                     :          0%
```

webfilter status

Use this command to display FortiGate Web Filtering rating information.

Syntax

```
get webfilter status [<refresh-rate_int>]
```

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
```

wireless-controller status

Use this command to list the physical AP (WTP) firmware images stored on the wireless-controller.

Syntax

```
get wireless-controller status
```