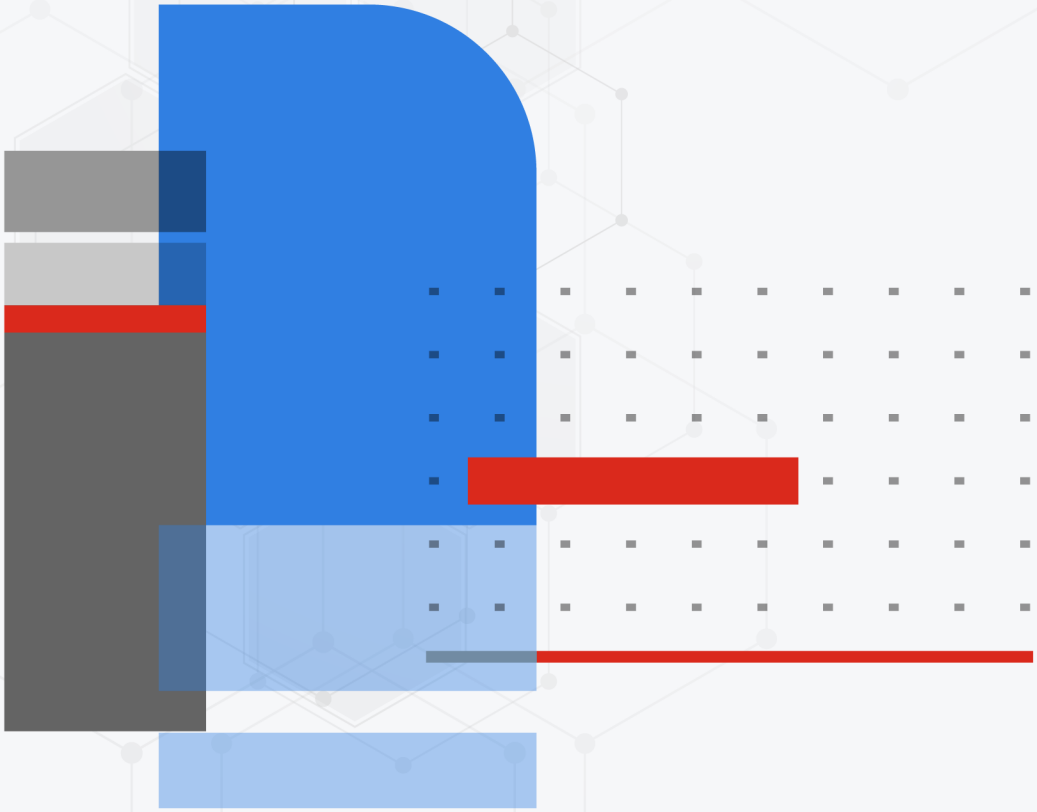
CLI Reference

Container FortiOS 7.2.1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 24, 2024
Container FortiOS 7.2.1 CLI Reference
87-721-976874-20240524

TABLE OF CONTENTS

Change Log ... **5**
Introduction ... **6**
Using the command line interface ... **7**
Connecting to the CLI ... 7
Command syntax ... 7
Notation ... 7
Optional values and ranges ... 8
CLI basics ... 8
Getting help ... 8
Shortcuts and key commands ... 9
Command abbreviation ... 9
Adding and removing options from lists ... 10
Environment variables ... 10
Special characters ... 10
Subcommands ... 11
next ... 11
end ... 12
Table subcommands ... 12
Field subcommands ... 14
CLI command reference ... **15**
config ... 15
antivirus ... 16
application ... 32
firewall ... 43
ips ... 110
log ... 121
report ... 154
router ... 155
system ... 157
vpn ... 174
webfilter ... 184
diagnose ... 206
diagnose autoupdate versions ... 206
diagnose debug ... 207
diagnose sniffer packet ... 208
diagnose sys ... 208
diagnose test application ... 210
execute ... 212
Syntax ... 212
Commands ... 213
exit ... 213
Usage ... 214
get ... 214
show ... 214

sysctl sh 215

Change Log

Date	Change Description
2024-05-24	Initial release.

Introduction

This document describes how to use the Container FortiOS command line interface (CLI) and contains references for Container FortiOS CLI commands.

The Container FortiOS CLI is similar to the FortiOS CLI. While much of the command syntax is the same, there are a limited number of commands available, reflecting the available Container FortiOS features.

Using the command line interface

This chapter explains how to connect to the CLI and describes the basics of using the CLI to configure and manage a running Container FortiOS container.

This chapter describes:

- Connecting to the CLI on page 7
- CLI basics on page 8
- Command syntax on page 7
- Subcommands on page 11

Connecting to the CLI

To connect to the running Container FortiOS container:

1. In the host shell, enter the appropriate command for your platform:
   - LXC: `lxc-console -n <container_name>`
   - Docker: `docker exec -it <container_name> /bin/cli`
   - Kubernetes: `kubectl exec --stdin --tty <container_name> /bin/cli`
2. At the prompt, enter the username and password.
   The default user is `admin` and the password is blank. See config system admin on page 157.

Command syntax

When entering a command, the CLI console requires that you use valid syntax and conform to expected input constraints. It rejects invalid commands. Indentation is used to indicate the levels of nested commands.

Each command line consists of a command word, usually followed by configuration data or a specific item that the command uses or affects.

Notation

Brackets, vertical bars, and spaces are used to denote valid syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

All syntax uses the following conventions:

Angle brackets < >	Indicate a variable of the specified data type.
Curly brackets { }	Indicate that a variable or variables are mandatory.

Square brackets [ ]	Indicate that the variable or variables are optional. For example: `show system interface [<name_str>]` To show the settings for all interfaces, you can enter `show system interface` To show the settings for the Port1 interface, you can enter `show system interface port1`.
Vertical bar |	A vertical bar separates alternative, mutually exclusive options. For example: `set protocol {ftp | sftp}` You can enter either `set protocol ftp` or `set protocol sftp`.

Space	A space separates non-mutually exclusive options.
	For example:
	`set allowaccess {ping https ssh snmp http fgfm radius-acct probe-response capwap ftm}`
	You can enter any of the following:
	`set allowaccess ping`
	`set allowaccess https ping ssh`
	`set allowaccess http https snmp ssh ping`
	In most cases, to make changes to lists that contain options separated by spaces, you need to retype the entire list, including all the options that you want to apply and excluding all the options that you want to remove.

Optional values and ranges

Any field that is optional will use square-brackets. The overall config command will still be valid whether or not the option is configured.

Square-brackets can be used is to show that multiple options can be set, even intermixed with ranges. The following example shows a field that can be set to either a specific value or range, or multiple instances:

```
config firewall service custom
    set iprange <range1> [<range2> <range3> ...]
end
```

CLI basics

This section describes the basic features and characteristics of the CLI environment.

Getting help

Press the question mark (?) key to display command help and complete commands.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.

- Enter a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Enter a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.
- Enter a question mark after entering a portion of a command to see a list of valid complete commands and their descriptions. If there is only one valid command, it will be automatically filled in.

Shortcuts and key commands

Shortcut key	Action
?	List valid complete or subsequent commands. If multiple commands can complete the command, they are listed with their descriptions.
Tab	Complete the word with the next available match. Press multiple times to cycle through available matches.
Up arrow or Ctrl + P	Recall the previous command. Command memory is limited to the current session.
Down arrow, or Ctrl + N	Recall the next command.
Left or Right arrow	Move the cursor left or right within the command line.
Ctrl + A	Move the cursor to the beginning of the command line.
Ctrl + E	Move the cursor to the end of the command line.
Ctrl + B	Move the cursor backwards one word.
Ctrl + F	Move the cursor forwards one word.
Ctrl + D	Delete the current character.
Ctrl + C	Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.
\ then Enter	Continue typing a command on the next line for a multiline command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command, enter a space instead of a backslash, and then press *Enter*.

Command abbreviation

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

For example, the command `diagnose system status` could be abbreviated to `d sy s`.

Adding and removing options from lists

When configuring a list, the `set` command will remove the previous configuration.

For example, if a user group currently includes members A, B, and C, the command `set member D` will remove members A, B, and C. To avoid removing the existing members from the group, the command `set members A B C D` must be used.

To avoid this issue, the following commands are available:

append	Add an option to an existing list. For example, `append member D` adds user D to the user group without removing any of the existing members.
select	Clear all of the options except for those specified. For example, `select member B` removes all member from the group except for member B.
unselect	Remove an option from an existing list. For example, `unselect member C` removes only member C from the group, without affecting the other members.

Environment variables

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

$USERFROM	The management access type (`ssh`, `jsconsole`, and so on) and the IPv4 address of the administrator that configured the item.
$USERNAME	The account name of the administrator that configured the item.
$SerialNum	The Container FortiOS serial number.

For example, to set the Container FortiOS host name to its serial number, use the following CLI command:

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

Special characters

The following characters cannot be used in most CLI commands: `<`, `>`, `(`, `)`, `#`, `'`, and `"`

If one of those characters, or a space, needs to be entered as part of a string, it can be entered by using a special command, enclosing the entire string in quotes, or preceding it with an escape character (backslash, \).

To enter a question mark (`?`) or a tab, *Ctrl* + *V* or *Ctrl* + *Shift* + - (depending on the method being used to access the CLI) must be entered first.

Question marks and tabs cannot be copied into the CLI Console or some SSH clients. They must be typed in.

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

Subcommands

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

```
config system fortiguard
```

the command prompt becomes:

```
(fortiguard)#
```

Applicable subcommands are available until you exit the command, or descend an additional level into another subcommand. Subcommand scope is indicated by indentation.

For example, the `edit` subcommand is only available in commands that affects tables, and the `next` subcommand is available only in the `edit` subcommand:

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

The available subcommands vary by command. From a command prompt under the `config` command, subcommands that affect tables and fields could be available.

next

The `next` command is used to maintain a hierarchy and flow to CLI commands. It is at the same indentation level as the preceding `edit` command, to mark where a table entry finishes.

The following example shows the next command used in the subcommand `entries`:

```
config application list
    edit default
        config entries
            edit 1
                set action pass
            next
```

After configuring table entry <1> then entering next, the <1> table entry is saved and the console returns to the entries prompt:

```
(entries) #
```

You can now create more table entries as needed, or enter end to save the table and return to the default table element prompt.

end

The end command is used to maintain a hierarchy and flow to CLI commands.

The following example shows the same command and subcommand as the next command example, except end has been entered instead of next after the subcommand:

```
config application list
    edit default
        config entries
            edit 1
                set action pass
        end
```

Entering end will save the <1> table entry and the table, and exit the entries subcommand entirely. The console returns to the default table element prompt:

```
(default) #
```

Table subcommands

edit <table_row>	Create or edit a table value.
	In objects such as security policies, <table_row> is a sequence number. To create a new table entry without accidentally editing an existing entry, enter edit 0. The CLI will confirm that creation of entry 0, but will assign the next unused number when the entry is saved after entering end or next.
	For example, to create a new firewall policy, enter the following commands:
	`config firewall policy`
	`    edit 0`
	`        ...`
	`    next`
	`end`
	To edit an existing policy, enter the following commands:
	`config firewall policy`
	`    edit 27`

	... next end The `edit` subcommand changes the command prompt to the name of the table value that is being edited, such as `(27) #`.

delete <table_row>	Delete a table value.
	For example, to delete firewall policy 27, enter the following commands:
	`config firewall policy`
	`delete 27`
	`end`

purge	Clear all table values. The `purge` command cannot be undone. To restore purged table values, the configuration must be restored from a backup.

move	Move an ordered table value.
	In the firewall policy table, this is equivalent to dragging a policy into a new position. It does not change the policy's ID number.
	For example, to move policy 27 to policy 30, enter the following commands:
	`config firewall policy`
	`move 27 to 30`
	`end`
	The `move` subcommand is only available in tables where the order of the table entries matters.

clone <table_row> to <table_row>	Make a clone of a table entry.
	For example, to create firewall policy 30 as a clone of policy 27, enter the following commands:
	`config firewall policy`
	`clone 27 to 30`
	`end`
	The `clone` subcommand may not be available for all tables.

rename <table_row> to <table_row>	Rename a table entry.
	For example to rename an administrator from Fry to Leela, enter the following commands:
	`config system admin`
	`rename Fry to Leela`
	`end`
	The `rename` subcommand is only available in tables where the entries can be renamed.

get	List the current table entries. For example, to view the existing firewall policy table entries, enter the following commands:

	`config firewall policy` `get`
show	Show the configuration. Only table entries that are not set to default values are shown.
end	Save the configuration and exit the current `config` command.

Purging the `system interface` or `system admin` tables does not reset default table values. You may be unable to connect to or log in to Container FortiOS.

Field subcommands

set <field> <value>	Modify the value of a field. For example, the command `set fsso enable` sets the `fsso` field to the value `enable`.
unset	Set the field to its default value.
clear	Clear all the options from a multi-option table value.
get	List the configuration of the current table entry, including default and customized values.
show	Show the configuration. Only values that are not set to default values are shown.
next	Save changes to the table entry and exit the `edit` command so that you can configure the next table entry.
abort	Exit the command without saving.
end	Save the configuration and exit the current `config` command.

CLI command reference

The following primary commands are available in Container FortiOS:

- config on page 15
- diagnose on page 206
- execute on page 212
- exit on page 213
- get on page 214
- show on page 214
- sysctl sh on page 215

config

Configure and manage Container FortiOS.

- antivirus on page 16
- application on page 32
- firewall on page 43
- ips on page 110
- log on page 121
- report on page 154
- router on page 155
- system on page 157
- vpn on page 174
- webfilter on page 184

antivirus

This section includes syntax for the following commands:

- config antivirus profile on page 16
- config antivirus settings on page 30

config antivirus profile

Configure AntiVirus profiles.

Syntax

```
config antivirus profile
    edit <name>
        set av-block-log [enable|disable]
        set av-virus-log [enable|disable]
        config cifs
            Description: Configure CIFS AntiVirus options.
            set archive-block {option1}, {option2}, ...
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
        end
        set comment {var-string}
        set extended-log [enable|disable]
        set ftgd-analytics [disable|suspicious|...]
        config ftp
            Description: Configure FTP AntiVirus options.
            set archive-block {option1}, {option2}, ...
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
        end
        config http
            Description: Configure HTTP AntiVirus options.
            set archive-block {option1}, {option2}, ...
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
        end
        config imap
            Description: Configure IMAP AntiVirus options.
            set archive-block {option1}, {option2}, ...
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
            set executables [default|virus]
        end
        config mapi
            Description: Configure MAPI AntiVirus options.
            set archive-block {option1}, {option2}, ...
```

```
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
            set executables [default|virus]
        end
        config nntp
            Description: Configure NNTP AntiVirus options.
            set archive-block {option1}, {option2}, ...
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
        end
        config pop3
            Description: Configure POP3 AntiVirus options.
            set archive-block {option1}, {option2}, ...
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
            set executables [default|virus]
        end
        set replacemsg-group {string}
        set scan-mode {option}
        config smtp
            Description: Configure SMTP AntiVirus options.
            set archive-block {option1}, {option2}, ...
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
            set executables [default|virus]
        end
        config ssh
            Description: Configure SFTP and SCP AntiVirus options.
            set archive-block {option1}, {option2}, ...
            set archive-log {option1}, {option2}, ...
            set av-scan [disable|block|...]
            set emulator [enable|disable]
        end
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
av-block-log	Enable/disable logging for AntiVirus file blocking.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
av-virus-log	Enable/disable AntiVirus logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
comment	Comment.	var-string	Maximum length: 255	
extended-log	Enable/disable extended logging for antivirus.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
ftgd-analytics	Settings to control which files are uploaded to FortiSandbox.	option	-	disable
	Option **Description** *disable* Do not upload files to FortiSandbox. *suspicious* Submit files supported by FortiSandbox if heuristics or other methods determine they are suspicious. *everything* Submit all files scanned by AntiVirus to FortiSandbox. AntiVirus may not scan all files.			
name	Profile name.	string	Maximum length: 35	
replacemsg-group	Replacement message group customized for this profile.	string	Maximum length: 35	
scan-mode	Choose between default scan mode and legacy scan mode.	option	-	default
	Option **Description** *default* On the fly decompression and scanning of certain archive files.			

config cifs

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option **Description** *encrypted* Block encrypted archives.			

Parameter	Description	Type	Size	Default
	Option / **Description** *corrupted* — Block corrupted archives. *partiallycorrupted* — Block partially corrupted archives. *multipart* — Block multipart archives. *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *fileslimit* — Block exceeded archive files limit. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiOS cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *fileslimit* — Log exceeded archive files limit. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiOS cannot open.			
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			

config ftp

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	

Option	Description
encrypted	Block encrypted archives.
corrupted	Block corrupted archives.
partiallycorrupted	Block partially corrupted archives.
multipart	Block multipart archives.
nested	Block nested archives that exceed uncompressed nest limit.
mailbomb	Block mail bomb archives.
fileslimit	Block exceeded archive files limit.
timeout	Block scan timeout.
unhandled	Block archives that FortiOS cannot open.

archive-log	Select the archive types to log.	option	-	

Option	Description
encrypted	Log encrypted archives.
corrupted	Log corrupted archives.
partiallycorrupted	Log partially corrupted archives.
multipart	Log multipart archives.
nested	Log nested archives that exceed uncompressed nest limit.
mailbomb	Log mail bomb archives.
fileslimit	Log exceeded archive files limit.
timeout	Log scan timeout.
unhandled	Log archives that FortiOS cannot open.

av-scan	Enable AntiVirus scan service.	option	-	disable

Option	Description
disable	Disable.
block	Block the virus infected files.
monitor	Log the virus infected files.

emulator	Enable/disable the virus emulator.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable the virus emulator. *disable* Disable the virus emulator.			

config http

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option **Description** *encrypted* Block encrypted archives. *corrupted* Block corrupted archives. *partiallycorrupted* Block partially corrupted archives. *multipart* Block multipart archives. *nested* Block nested archives that exceed uncompressed nest limit. *mailbomb* Block mail bomb archives. *fileslimit* Block exceeded archive files limit. *timeout* Block scan timeout. *unhandled* Block archives that FortiOS cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option **Description** *encrypted* Log encrypted archives. *corrupted* Log corrupted archives. *partiallycorrupted* Log partially corrupted archives. *multipart* Log multipart archives. *nested* Log nested archives that exceed uncompressed nest limit. *mailbomb* Log mail bomb archives. *fileslimit* Log exceeded archive files limit. *timeout* Log scan timeout. *unhandled* Log archives that FortiOS cannot open.			
av-scan	Enable AntiVirus scan service.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable. *block* Block the virus infected files. *monitor* Log the virus infected files.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option **Description** *enable* Enable the virus emulator. *disable* Disable the virus emulator.			

config imap

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option **Description** *encrypted* Block encrypted archives. *corrupted* Block corrupted archives. *partiallycorrupted* Block partially corrupted archives. *multipart* Block multipart archives. *nested* Block nested archives that exceed uncompressed nest limit. *mailbomb* Block mail bomb archives. *fileslimit* Block exceeded archive files limit. *timeout* Block scan timeout. *unhandled* Block archives that FortiOS cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option **Description** *encrypted* Log encrypted archives. *corrupted* Log corrupted archives. *partiallycorrupted* Log partially corrupted archives. *multipart* Log multipart archives. *nested* Log nested archives that exceed uncompressed nest limit.			

Parameter	Description	Type	Size	Default
	Option **Description** *mailbomb* Log mail bomb archives. *fileslimit* Log exceeded archive files limit. *timeout* Log scan timeout. *unhandled* Log archives that FortiOS cannot open.			
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option **Description** *disable* Disable. *block* Block the virus infected files. *monitor* Log the virus infected files.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option **Description** *enable* Enable the virus emulator. *disable* Disable the virus emulator.			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option **Description** *default* Perform standard AntiVirus scanning of Windows executable files. *virus* Treat Windows executables as viruses.			

config mapi

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option **Description** *encrypted* Block encrypted archives. *corrupted* Block corrupted archives. *partiallycorrupted* Block partially corrupted archives. *multipart* Block multipart archives.			

Parameter	Description	Type	Size	Default
	Option / **Description** *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *fileslimit* — Block exceeded archive files limit. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiOS cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *fileslimit* — Log exceeded archive files limit. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiOS cannot open.			
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default

Parameter	Description	Type	Size	Default

Option	Description
default	Perform standard AntiVirus scanning of Windows executable files.
virus	Treat Windows executables as viruses.

config nntp

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	

Option	Description
encrypted	Block encrypted archives.
corrupted	Block corrupted archives.
partiallycorrupted	Block partially corrupted archives.
multipart	Block multipart archives.
nested	Block nested archives that exceed uncompressed nest limit.
mailbomb	Block mail bomb archives.
fileslimit	Block exceeded archive files limit.
timeout	Block scan timeout.
unhandled	Block archives that FortiOS cannot open.

archive-log	Select the archive types to log.	option	-	

Option	Description
encrypted	Log encrypted archives.
corrupted	Log corrupted archives.
partiallycorrupted	Log partially corrupted archives.
multipart	Log multipart archives.
nested	Log nested archives that exceed uncompressed nest limit.
mailbomb	Log mail bomb archives.
fileslimit	Log exceeded archive files limit.
timeout	Log scan timeout.
unhandled	Log archives that FortiOS cannot open.

av-scan	Enable AntiVirus scan service.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable. *block* Block the virus infected files. *monitor* Log the virus infected files.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option **Description** *enable* Enable the virus emulator. *disable* Disable the virus emulator.			

config pop3

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option **Description** *encrypted* Block encrypted archives. *corrupted* Block corrupted archives. *partiallycorrupted* Block partially corrupted archives. *multipart* Block multipart archives. *nested* Block nested archives that exceed uncompressed nest limit. *mailbomb* Block mail bomb archives. *fileslimit* Block exceeded archive files limit. *timeout* Block scan timeout. *unhandled* Block archives that FortiOS cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option **Description** *encrypted* Log encrypted archives. *corrupted* Log corrupted archives. *partiallycorrupted* Log partially corrupted archives. *multipart* Log multipart archives. *nested* Log nested archives that exceed uncompressed nest limit.			

Parameter	Description	Type	Size	Default
	Option **Description** *mailbomb* Log mail bomb archives. *fileslimit* Log exceeded archive files limit. *timeout* Log scan timeout. *unhandled* Log archives that FortiOS cannot open.			
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option **Description** *disable* Disable. *block* Block the virus infected files. *monitor* Log the virus infected files.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option **Description** *enable* Enable the virus emulator. *disable* Disable the virus emulator.			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default
	Option **Description** *default* Perform standard AntiVirus scanning of Windows executable files. *virus* Treat Windows executables as viruses.			

config smtp

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	
	Option **Description** *encrypted* Block encrypted archives. *corrupted* Block corrupted archives. *partiallycorrupted* Block partially corrupted archives. *multipart* Block multipart archives.			

Parameter	Description	Type	Size	Default
	Option / **Description** *nested* — Block nested archives that exceed uncompressed nest limit. *mailbomb* — Block mail bomb archives. *fileslimit* — Block exceeded archive files limit. *timeout* — Block scan timeout. *unhandled* — Block archives that FortiOS cannot open.			
archive-log	Select the archive types to log.	option	-	
	Option / **Description** *encrypted* — Log encrypted archives. *corrupted* — Log corrupted archives. *partiallycorrupted* — Log partially corrupted archives. *multipart* — Log multipart archives. *nested* — Log nested archives that exceed uncompressed nest limit. *mailbomb* — Log mail bomb archives. *fileslimit* — Log exceeded archive files limit. *timeout* — Log scan timeout. *unhandled* — Log archives that FortiOS cannot open.			
av-scan	Enable AntiVirus scan service.	option	-	disable
	Option / **Description** *disable* — Disable. *block* — Block the virus infected files. *monitor* — Log the virus infected files.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option / **Description** *enable* — Enable the virus emulator. *disable* — Disable the virus emulator.			
executables	Treat Windows executable files as viruses for the purpose of blocking or monitoring.	option	-	default

Parameter	Description	Type	Size	Default

Option	Description
default	Perform standard AntiVirus scanning of Windows executable files.
virus	Treat Windows executables as viruses.

config ssh

Parameter	Description	Type	Size	Default
archive-block	Select the archive types to block.	option	-	

Option	Description
encrypted	Block encrypted archives.
corrupted	Block corrupted archives.
partiallycorrupted	Block partially corrupted archives.
multipart	Block multipart archives.
nested	Block nested archives that exceed uncompressed nest limit.
mailbomb	Block mail bomb archives.
fileslimit	Block exceeded archive files limit.
timeout	Block scan timeout.
unhandled	Block archives that FortiOS cannot open.

archive-log	Select the archive types to log.	option	-	

Option	Description
encrypted	Log encrypted archives.
corrupted	Log corrupted archives.
partiallycorrupted	Log partially corrupted archives.
multipart	Log multipart archives.
nested	Log nested archives that exceed uncompressed nest limit.
mailbomb	Log mail bomb archives.
fileslimit	Log exceeded archive files limit.
timeout	Log scan timeout.
unhandled	Log archives that FortiOS cannot open.

av-scan	Enable AntiVirus scan service.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable. *block* Block the virus infected files. *monitor* Log the virus infected files.			
emulator	Enable/disable the virus emulator.	option	-	enable
	Option **Description** *enable* Enable the virus emulator. *disable* Disable the virus emulator.			

config antivirus settings

Configure AntiVirus settings.

Syntax

```
config antivirus settings
    set grayware [enable|disable]
    set machine-learning-detection [enable|monitor|...]
    set override-timeout {integer}
    set use-extreme-db [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
grayware	Enable/disable grayware detection when an AntiVirus profile is applied to traffic.	option	-	disable
	Option **Description** *enable* Enable grayware detection. *disable* Disable grayware detection.			
machine-learning-detection	Use machine learning based malware detection.	option	-	enable
	Option **Description** *enable* Enable machine learning based malware detection.			

Parameter	Description	Type	Size	Default
	Option / **Description** *monitor* — Enable machine learning based malware detection for monitoring only. *disable* — Disable machine learning based malware detection.			
override-timeout	Override the large file scan timeout value in seconds. Zero is the default value and is used to disable this command. When disabled, the daemon adjusts the large file scan timeout based on the file size.	integer	Minimum value: 30 Maximum value: 3600	0
use-extreme-db	Enable/disable the use of Extreme AVDB.	option	-	disable
	Option / **Description** *enable* — Enable extreme AVDB. *disable* — Disable extreme AVDB.			

application

This section includes syntax for the following commands:

- config application group on page 32
- config application list on page 33
- config application name on page 42

config application group

Configure firewall application groups.

Syntax

```
config application group
    edit <name>
        set application <id1>, <id2>, ...
        set behavior {user}
        set category <id1>, <id2>, ...
        set comment {var-string}
        set popularity {option1}, {option2}, ...
        set protocols {user}
        set risk <level1>, <level2>, ...
        set technology {user}
        set type [application|filter]
        set vendor {user}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
behavior	Application behavior filter.	user	Not Specified	all
category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
comment	Comment	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
name	Application group name.	string	Maximum length: 63	
popularity	Application popularity filter.	option	-	1 2 3 4 5
	Option / **Description** *1* — Popularity level 1. *2* — Popularity level 2. *3* — Popularity level 3. *4* — Popularity level 4. *5* — Popularity level 5.			
protocols	Application protocol filter.	user	Not Specified	all
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295	
technology	Application technology filter.	user	Not Specified	all
type	Application group type.	option	-	application
	Option / **Description** *application* — Application ID. *filter* — Application filter.			
vendor	Application vendor filter.	user	Not Specified	all

config application list

Configure application control lists.

Syntax

```
config application list
    edit <name>
        set app-replacemsg [disable|enable]
        set comment {var-string}
        set control-default-network-services [disable|enable]
        set deep-app-inspection [disable|enable]
        config default-network-services
            Description: Default network service entries.
            edit <id>
                set port {integer}
```

```
            set services {option1}, {option2}, ...
            set violation-action [pass|monitor|...]
        next
    end
    set enforce-default-app-port [disable|enable]
    config entries
        Description: Application list entries.
        edit <id>
            set action [pass|block|...]
            set application <id1>, <id2>, ...
            set behavior {user}
            set category <id1>, <id2>, ...
            set exclusion <id1>, <id2>, ...
            set log [disable|enable]
            set log-packet [disable|enable]
            config parameters
                Description: Application parameters.
                edit <id>
                    config members
                        Description: Parameter tuple members.
                        edit <id>
                            set name {string}
                            set value {string}
                        next
                    end
                next
            end
            set per-ip-shaper {string}
            set popularity {option1}, {option2}, ...
            set protocols {user}
            set quarantine [none|attacker]
            set quarantine-expiry {user}
            set quarantine-log [disable|enable]
            set rate-count {integer}
            set rate-duration {integer}
            set rate-mode [periodical|continuous]
            set rate-track [none|src-ip|...]
            set risk <level1>, <level2>, ...
            set session-ttl {integer}
            set shaper {string}
            set shaper-reverse {string}
            set technology {user}
            set vendor {user}
        next
    end
    set extended-log [enable|disable]
    set force-inclusion-ssl-di-sigs [disable|enable]
    set options {option1}, {option2}, ...
    set other-application-action [pass|block]
    set other-application-log [disable|enable]
    set p2p-block-list {option1}, {option2}, ...
    set replacemsg-group {string}
    set unknown-application-action [pass|block]
    set unknown-application-log [disable|enable]
next
end
```

Parameters

Parameter	Description	Type	Size	Default
app-replacemsg	Enable/disable replacement messages for blocked applications.	option	-	enable
	Option / **Description** *disable* — Disable replacement messages for blocked applications. *enable* — Enable replacement messages for blocked applications.			
comment	comments	var-string	Maximum length: 255	
control-default-network-services	Enable/disable enforcement of protocols over selected ports.	option	-	disable
	Option / **Description** *disable* — Disable protocol enforcement over selected ports. *enable* — Enable protocol enforcement over selected ports.			
deep-app-inspection	Enable/disable deep application inspection.	option	-	enable
	Option / **Description** *disable* — Disable deep application inspection. *enable* — Enable deep application inspection.			
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	disable
	Option / **Description** *disable* — Disable default application port enforcement. *enable* — Enable default application port enforcement.			
extended-log	Enable/disable extended logging.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			

Parameter	Description	Type	Size	Default
force-inclusion-ssl-di-sigs	Enable/disable forced inclusion of SSL deep inspection signatures.	option	-	disable
	Option / **Description** *disable* — Disable forced inclusion of signatures which normally require SSL deep inspection. *enable* — Enable forced inclusion of signatures which normally require SSL deep inspection.			
name	List name.	string	Maximum length: 35	
options	Basic application protocol signatures allowed by default.	option	-	allow-dns
	Option / **Description** *allow-dns* — Allow DNS. *allow-icmp* — Allow ICMP. *allow-http* — Allow generic HTTP web browsing. *allow-ssl* — Allow generic SSL communication. *allow-quic* — Allow QUIC.			
other-application-action	Action for other applications.	option	-	pass
	Option / **Description** *pass* — Allow sessions matching an application in this application list. *block* — Block sessions matching an application in this application list.			
other-application-log	Enable/disable logging for other applications.	option	-	disable
	Option / **Description** *disable* — Disable logging for other applications. *enable* — Enable logging for other applications.			
p2p-block-list	P2P applications to be blocklisted.	option	-	

Parameter	Description	Type	Size	Default
	Option **Description** *skype* Skype. *edonkey* Edonkey. *bittorrent* Bit torrent.			
replacemsg-group	Replacement message group.	string	Maximum length: 35	
unknown-application-action	Pass or block traffic from unknown applications.	option	-	pass
	Option **Description** *pass* Pass or allow unknown applications. *block* Drop or block unknown applications.			
unknown-application-log	Enable/disable logging for unknown applications.	option	-	disable
	Option **Description** *disable* Disable logging for unknown applications. *enable* Enable logging for unknown applications.			

config default-network-services

Parameter	Description	Type	Size	Default
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
port	Port number.	integer	Minimum value: 0 Maximum value: 65535	0
services	Network protocols.	option	-	
	Option **Description** *http* HTTP.			

Parameter	Description	Type	Size	Default
	Option / **Description** *ssh* — SSH. *telnet* — TELNET. *ftp* — FTP. *dns* — DNS. *smtp* — SMTP. *pop3* — POP3. *imap* — IMAP. *snmp* — SNMP. *nntp* — NNTP. *https* — HTTPS.			
violation-action	Action for protocols not in the allowlist for selected port. **Option** / **Description** *pass* — Allow protocols not in the allowlist for selected port. *monitor* — Monitor protocols not in the allowlist for selected port. *block* — Block protocols not in the allowlist for selected port.	option	-	block

config entries

Parameter	Description	Type	Size	Default
action	Pass or block traffic, or reset connection for traffic from this application. **Option** / **Description** *pass* — Pass or allow matching traffic. *block* — Block or drop matching traffic. *reset* — Reset sessions for matching traffic.	option	-	block
application <id>	ID of allowed applications. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	

Parameter	Description	Type	Size	Default
behavior	Application behavior filter.	user	Not Specified	all
category <id>	Category ID list. Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	
exclusion <id>	ID of excluded applications. Excluded application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
log	Enable/disable logging for this application list.	option	-	enable

Option	Description
disable	Disable logging.
enable	Enable logging.

log-packet	Enable/disable packet logging.	option	-	disable

Option	Description
disable	Disable packet logging.
enable	Enable packet logging.

per-ip-shaper	Per-IP traffic shaper.	string	Maximum length: 35	
popularity	Application popularity filter.	option	-	1 2 3 4 5

Option	Description
1	Popularity level 1.
2	Popularity level 2.
3	Popularity level 3.
4	Popularity level 4.
5	Popularity level 5.

Parameter	Description	Type	Size	Default
protocols	Application protocol filter.	user	Not Specified	all
quarantine	Quarantine method.	option	-	none

Option	Description
none	Quarantine is disabled.
attacker	Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.

Parameter	Description	Type	Size	Default
quarantine-expiry	Duration of quarantine. Requires quarantine set to attacker.	user	Not Specified	5m
quarantine-log	Enable/disable quarantine logging.	option	-	enable

Option	Description
disable	Disable quarantine logging.
enable	Enable quarantine logging.

Parameter	Description	Type	Size	Default
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60
rate-mode	Rate limit mode.	option	-	continuous

Option	Description
periodical	Allow configured number of packets every rate-duration.
continuous	Block packets once the rate is reached.

Parameter	Description	Type	Size	Default
rate-track	Track the packet protocol field.	option	-	none

Option	Description
none	none
src-ip	Source IP.
dest-ip	Destination IP.
dhcp-client-mac	DHCP client.
dns-domain	DNS domain.

Parameter	Description	Type	Size	Default
risk <level>	Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical). Risk, or impact, of allowing traffic from this application to occur (1 - 5; Low, Elevated, Medium, High, and Critical).	integer	Minimum value: 0 Maximum value: 4294967295	
session-ttl	Session TTL.	integer	Minimum value: 0 Maximum value: 4294967295	0
shaper	Traffic shaper.	string	Maximum length: 35	
shaper-reverse	Reverse traffic shaper.	string	Maximum length: 35	
technology	Application technology filter.	user	Not Specified	all
vendor	Application vendor filter.	user	Not Specified	all

config parameters

Parameter	Description	Type	Size	Default
id	Parameter tuple ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config members

Parameter	Description	Type	Size	Default
id	Parameter.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Parameter name.	string	Maximum length: 31	
value	Parameter value.	string	Maximum length: 199	

config application name

Configure application signatures. Read-only.

This table cannot be edited.

Syntax

```
config application name
    edit <name>
        get
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
behavior	Application behavior.	user	Not Specified	
category	Application category ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
id	Application ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Application name.	string	Maximum length: 63	
popularity	Application popularity.	integer	Minimum value: 0 Maximum value: 255	0
protocol	Application protocol.	user	Not Specified	
risk	Application risk.	integer	Minimum value: 0 Maximum value: 255	0
technology	Application technology.	user	Not Specified	
vendor	Application vendor.	user	Not Specified	
weight	Application weight.	integer	Minimum value: 0 Maximum value: 255	0

firewall

This section includes syntax for the following commands:

- config firewall address on page 43
- config firewall addrgrp on page 44
- config firewall central-snat-map on page 45
- config firewall policy on page 47
- config firewall profile-protocol-options on page 50
- config firewall schedule group on page 72
- config firewall schedule onetime on page 72
- config firewall schedule recurring on page 73
- config firewall security-policy on page 74
- config firewall service category on page 79
- config firewall service custom on page 79
- config firewall service group on page 82
- config firewall ssl-ssh-profile on page 82
- config firewall vip on page 106
- config firewall wildcard-fqdn custom on page 108

config firewall address

Configure IPv4 addresses.

Syntax

```
config firewall address
    edit <name>
        set comment {var-string}
        set end-ip {ipv4-address-any}
        set start-ip {ipv4-address-any}
        set subnet {ipv4-classnet-any}
        set type [ipmask|iprange]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
end-ip	Final IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
name	Address name.	string	Maximum length: 79	
start-ip	First IP address (inclusive) in the range for the address.	ipv4-address-any	Not Specified	0.0.0.0
subnet	IP address and subnet mask of address.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0
type	Type of address.	option	-	ipmask

Option	Description
ipmask	Standard IPv4 address with subnet mask.
iprange	Range of IPv4 addresses between two specified addresses (inclusive).

config firewall addrgrp

Configure IPv4 address groups.

Syntax

```
config firewall addrgrp
    edit <name>
        set category [default|ztna-ems-tag|...]
        set comment {var-string}
        set exclude [enable|disable]
        set exclude-member <name1>, <name2>, ...
        set member <name1>, <name2>, ...
        set type [default|folder]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
category	Address group category.	option	-	default

Option	Description
default	Default address group category (cannot be used as ztna-ems-tag/ztna-geo-tag in policy).
ztna-ems-tag	Members must be ztna-ems-tag group or ems-tag address, can be used as ztna-ems-tag in policy.

Parameter	Description	Type	Size	Default
	Option / **Description** *ztna-geo-tag* / Members must be ztna-geo-tag group or geographic address, can be used as ztna-geo-tag in policy.			
comment	Comment.	var-string	Maximum length: 255	
exclude	Enable/disable address exclusion.	option	-	disable
	Option / **Description** *enable* / Enable address exclusion. *disable* / Disable address exclusion.			
exclude-member <name>	Address exclusion member. Address name.	string	Maximum length: 79	
member <name>	Address objects contained within the group. Address name.	string	Maximum length: 79	
name	Address group name.	string	Maximum length: 79	
type	Address group type.	option	-	default
	Option / **Description** *default* / Default address group type (address may belong to multiple groups). *folder* / Address folder group (members may not belong to any other group).			

config firewall central-snat-map

Configure IPv4 and IPv6 central SNAT policies.

Syntax

```
config firewall central-snat-map
    edit <policyid>
        set comments {var-string}
        set dst-addr <name1>, <name2>, ...
        set dst-addr6 <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set nat [disable|enable]
        set nat-ippool <name1>, <name2>, ...
        set nat-ippool6 <name1>, <name2>, ...
        set nat-port {user}
        set orig-addr <name1>, <name2>, ...
        set orig-addr6 <name1>, <name2>, ...
```

```
        set orig-port {user}
        set protocol {integer}
        set srcintf <name1>, <name2>, ...
        set status [enable|disable]
        set type [ipv4|ipv6]
    next
end
```

config firewall central-snat-map

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	
dst-addr <name>	IPv4 Destination address. Address name.	string	Maximum length: 79	
dst-addr6 <name>	IPv6 Destination address. Address name.	string	Maximum length: 79	
dstintf <name>	Destination interface name from available interfaces. Interface name.	string	Maximum length: 79	
nat	Enable/disable source NAT.	option	-	enable
	Option / **Description** *disable* — Disable source NAT. *enable* — Enable source NAT.			
nat-ippool <name>	Name of the IP pools to be used to translate addresses from available IP Pools. IP pool name.	string	Maximum length: 79	
nat-ippool6 <name>	IPv6 pools to be used for source NAT. IPv6 pool name.	string	Maximum length: 79	
nat-port	Translated port or port range (1 to 65535, 0 means any port).	user	Not Specified	
orig-addr <name>	IPv4 Original address. Address name.	string	Maximum length: 79	
orig-addr6 <name>	IPv6 Original address. Address name.	string	Maximum length: 79	
orig-port	Original TCP port (1 to 65535, 0 means any port).	user	Not Specified	

Parameter	Description	Type	Size	Default
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
protocol	Integer value for the protocol type.	integer	Minimum value: 0 Maximum value: 255	0
srcintf <name>	Source interface name from available interfaces. Interface name.	string	Maximum length: 79	
status	Enable/disable the active status of this policy.	option	-	enable

Option	Description
enable	Enable this policy.
disable	Disable this policy.

type	IPv4/IPv6 source NAT.	option	-	ipv4

Option	Description
ipv4	Perform IPv4 source NAT.
ipv6	Perform IPv6 source NAT.

config firewall policy

Configure IPv4/IPv6 policies.

Syntax

```
config firewall policy
    edit <policyid>
        set action [accept|deny]
        set application-list {string}
        set av-profile {string}
        set comments {var-string}
        set custom-log-fields <field-id1>, <field-id2>, ...
        set dstaddr <name1>, <name2>, ...
        set dstaddr6 <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set ips-sensor {string}
        set logtraffic [all|utm|...]
        set name {string}
        set nat [enable|disable]
        set profile-group {string}
        set profile-protocol-options {string}
```

```
        set profile-type [single|group]
        set service <name1>, <name2>, ...
        set srcaddr <name1>, <name2>, ...
        set srcaddr6 <name1>, <name2>, ...
        set srcintf <name1>, <name2>, ...
        set ssl-ssh-profile {string}
        set status [enable|disable]
        set utm-status [enable|disable]
        set webfilter-profile {string}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
action	Policy action (accept/deny).	option	-	accept
	Option / **Description** *accept* — Allows session that match the firewall policy. *deny* — Blocks sessions that match the firewall policy.			
application-list	Name of an existing Application list.	string	Maximum length: 35	
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	
comments	Comment.	var-string	Maximum length: 1023	
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35	
dstaddr <name>	Destination IPv4 address and address group names. Address name.	string	Maximum length: 79	
dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm

Parameter	Description	Type	Size	Default
	Option **Description** *all* Log all sessions accepted or denied by this policy. *utm* Log traffic that has a security profile applied to it. *disable* Disable all logging for this policy.			
name	Policy name.	string	Maximum length: 35	
nat	Enable/disable source NAT.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
policyid	Policy ID.	integer	Minimum value: 1 Maximum value: 65535	1
profile-group	Name of profile group.	string	Maximum length: 35	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single
	Option **Description** *single* Do not allow security profile groups. *group* Allow security profile groups.			
service <name>	Service and service group names. Service and service group names.	string	Maximum length: 79	
srcaddr <name>	Source IPv4 address and address group names. Address name.	string	Maximum length: 79	
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79	
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
ssl-ssh-profile	Name of an existing SSL SSH profile.	string	Maximum length: 35	no-inspection
status	Enable or disable this policy.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
utm-status	Enable to add one or more security profiles (AV, IPS, etc.) to the firewall policy.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	

config firewall profile-protocol-options

Configure protocol options.

Syntax

```
config firewall profile-protocol-options
    edit <name>
        config cifs
            Description: Configure CIFS protocol options.
            set domain-controller {string}
            set options {option1}, {option2}, ...
            set oversize-limit {integer}
            set scan-bzip2 [enable|disable]
            set server-credential-type [none|credential-replication|...]
            config server-keytab
                Description: Server keytab.
                edit <principal>
                    set keytab {string}
                next
            end
            set status [enable|disable]
            set tcp-window-maximum {integer}
            set tcp-window-minimum {integer}
            set tcp-window-size {integer}
            set tcp-window-type [system|static|...]
            set uncompressed-nest-limit {integer}
            set uncompressed-oversize-limit {integer}
        end
        set comment {var-string}
```

```
config dns
    Description: Configure DNS protocol options.
    set status [enable|disable]
end
config ftp
    Description: Configure FTP protocol options.
    set comfort-amount {integer}
    set comfort-interval {integer}
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set stream-based-uncompressed-limit {integer}
    set tcp-window-maximum {integer}
    set tcp-window-minimum {integer}
    set tcp-window-size {integer}
    set tcp-window-type [system|static|...]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config http
    Description: Configure HTTP protocol options.
    set block-page-status-code {integer}
    set comfort-amount {integer}
    set comfort-interval {integer}
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set post-lang {option1}, {option2}, ...
    set proxy-after-tcp-handshake [enable|disable]
    set range-block [disable|enable]
    set retry-count {integer}
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set stream-based-uncompressed-limit {integer}
    set streaming-content-bypass [enable|disable]
    set strip-x-forwarded-for [disable|enable]
    set switching-protocols [bypass|block]
    set tcp-window-maximum {integer}
    set tcp-window-minimum {integer}
    set tcp-window-size {integer}
    set tcp-window-type [system|static|...]
    set tunnel-non-http [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
    set unknown-http-version [reject|tunnel|...]
end
config imap
    Description: Configure IMAP protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set proxy-after-tcp-handshake [enable|disable]
```

```
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config mail-signature
    Description: Configure Mail signature.
    set signature {string}
    set status [disable|enable]
end
config mapi
    Description: Configure MAPI protocol options.
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set scan-bzip2 [enable|disable]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
config nntp
    Description: Configure NNTP protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set scan-bzip2 [enable|disable]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
set oversize-log [disable|enable]
config pop3
    Description: Configure POP3 protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set scan-bzip2 [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
    set uncompressed-nest-limit {integer}
    set uncompressed-oversize-limit {integer}
end
set replacemsg-group {string}
set rpc-over-http [enable|disable]
config smtp
    Description: Configure SMTP protocol options.
    set inspect-all [enable|disable]
    set options {option1}, {option2}, ...
    set oversize-limit {integer}
    set proxy-after-tcp-handshake [enable|disable]
    set scan-bzip2 [enable|disable]
    set server-busy [enable|disable]
    set ssl-offloaded [no|yes]
    set status [enable|disable]
```

```
            set uncompressed-nest-limit {integer}
            set uncompressed-oversize-limit {integer}
        end
        config ssh
            Description: Configure SFTP and SCP protocol options.
            set comfort-amount {integer}
            set comfort-interval {integer}
            set options {option1}, {option2}, ...
            set oversize-limit {integer}
            set scan-bzip2 [enable|disable]
            set ssl-offloaded [no|yes]
            set stream-based-uncompressed-limit {integer}
            set tcp-window-maximum {integer}
            set tcp-window-minimum {integer}
            set tcp-window-size {integer}
            set tcp-window-type [system|static|...]
            set uncompressed-nest-limit {integer}
            set uncompressed-oversize-limit {integer}
        end
        set switching-protocols-log [disable|enable]
    next
end
```

config firewall profile-protocol-options

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
name	Name.	string	Maximum length: 35	
oversize-log	Enable/disable logging for antivirus oversize file blocking.	option	-	disable

Option	Description
disable	Disable logging for antivirus oversize file blocking.
enable	Enable logging for antivirus oversize file blocking.

Parameter	Description	Type	Size	Default
replacemsg-group	Name of the replacement message group to be used	string	Maximum length: 35	
rpc-over-http	Enable/disable inspection of RPC over HTTP.	option	-	disable

Option	Description
enable	Enable inspection of RPC over HTTP.
disable	Disable inspection of RPC over HTTP.

Parameter	Description	Type	Size	Default
switching-protocols-log	Enable/disable logging for HTTP/HTTPS switching protocols.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable logging for HTTP/HTTPS switching protocols. *enable* Enable logging for HTTP/HTTPS switching protocols.			

config cifs

Parameter	Description	Type	Size	Default
domain-controller	Domain for which to decrypt CIFS traffic.	string	Maximum length: 63	
options	One or more options that can be applied to the session. **Option** **Description** *oversize* Block oversized file/email.	option	-	
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10
scan-bzip2	Enable/disable scanning of BZip2 compressed files. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	enable
server-credential-type	CIFS server credential type. **Option** **Description** *none* Credential derivation not set. *credential-replication* Credential derived using Replication account on Domain Controller. *credential-keytab* Credential derived using server keytab.	option	-	none
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
tcp-window-type	TCP window type to use for this protocol.	option	-	system
	Option / **Description** *system* / Use system default TCP window size for this protocol (default). *static* / Manually specify TCP window size. *dynamic* / Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config server-keytab

Parameter	Description	Type	Size	Default
keytab	Base64 encoded keytab file containing credential of the server.	string	Maximum length: 8191	
principal	Service principal. For example, "host/cifsserver.example.com@example.com".	string	Maximum length: 511	

config dns

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

config ftp

Parameter	Description	Type	Size	Default
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data.	integer	Minimum value: 1 Maximum value: 900	10
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

options	One or more options that can be applied to the session.	option	-	

Parameter	Description	Type	Size	Default
	Option / **Description** *clientcomfort* — Prevent client timeout. *oversize* — Block oversized file/email. *splice* — Enable splice mode. *bypass-rest-command* — Bypass REST command. *bypass-mode-command* — Bypass MODE command.			
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10
scan-bzip2	Enable/disable scanning of BZip2 compressed files. **Option** / **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	enable
ssl-offloaded	SSL decryption and encryption performed by an external device. **Option** / **Description** *no* — SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled. *yes* — SSL decryption and encryption performed by an external device.	option	-	no
status	Enable/disable the active status of scanning for this protocol. **Option** / **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	enable
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
tcp-window-type	TCP window type to use for this protocol.	option	-	system

Option	Description
system	Use system default TCP window size for this protocol (default).
static	Manually specify TCP window size.
dynamic	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.

Parameter	Description	Type	Size	Default
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config http

Parameter	Description	Type	Size	Default
block-page-status-code	Code number returned for blocked HTTP pages.	integer	Minimum value: 100 Maximum value: 599	403

Parameter	Description	Type	Size	Default
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data.	integer	Minimum value: 1 Maximum value: 900	10
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

options	One or more options that can be applied to the session.	option	-	

Option	Description
clientcomfort	Prevent client timeout.
servercomfort	Prevent server timeout.
oversize	Block oversized file/email.
chunkedbypass	Bypass chunked transfer encoded sites.

oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10
post-lang	ID codes for character sets to be used to convert to UTF-8 for banned words and DLP on HTTP posts (maximum of 5 character sets).	option	-	

Option	Description
jisx0201	Japanese Industrial Standard 0201.
jisx0208	Japanese Industrial Standard 0208.
jisx0212	Japanese Industrial Standard 0212.
gb2312	Guojia Biaozhun 2312 (simplified Chinese).
ksc5601-ex	Wansung Korean standard 5601.
euc-jp	Extended Unicode Japanese.

Parameter	Description	Type	Size	Default
	Option / **Description** *sjis* — Shift Japanese Industrial Standard. *iso2022-jp* — ISO 2022 Japanese. *iso2022-jp-1* — ISO 2022-1 Japanese. *iso2022-jp-2* — ISO 2022-2 Japanese. *euc-cn* — Extended Unicode Chinese. *ces-gbk* — Extended GB2312 (simplified Chinese). *hz* — Hanzi simplified Chinese. *ces-big5* — Big-5 traditional Chinese. *euc-kr* — Extended Unicode Korean. *iso2022-jp-3* — ISO 2022-3 Japanese. *iso8859-1* — ISO 8859 Part 1 (Western European). *tis620* — Thai Industrial Standard 620. *cp874* — Code Page 874 (Thai). *cp1252* — Code Page 1252 (Western European Latin). *cp1251* — Code Page 1251 (Cyrillic).			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before). **Option** / **Description** *enable* — Enable setting. *disable* — Disable setting.	option	-	disable
range-block	Enable/disable blocking of partial downloads. **Option** / **Description** *disable* — Disable range header blocking (allow partial file downloads) *enable* — Enable range header blocking (treat all partial file downloads as full file download)	option	-	disable
retry-count	Number of attempts to retry HTTP connection.	integer	Minimum value: 0 Maximum value: 100	0

Parameter	Description	Type	Size	Default
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no

Option	Description
no	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.
yes	SSL decryption and encryption performed by an external device.

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned.	integer	Minimum value: 0 Maximum value: 4294967295	0
streaming-content-bypass	Enable/disable bypassing of streaming content from buffering.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
strip-x-forwarded-for	Enable/disable stripping of HTTP X-Forwarded-For header.	option	-	disable

Option	Description
disable	Disable changing of HTTP X-Forwarded-For header.
enable	Enable replacement of X-Forwarded-For value with 1.1.1.1.

Parameter	Description	Type	Size	Default
switching-protocols	Bypass from scanning, or block a connection that attempts to switch protocol.	option	-	bypass

Option	Description
bypass	Bypass connections when switching protocols.
block	Block connections when switching protocols.

tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
tcp-window-type	TCP window type to use for this protocol.	option	-	system

Option	Description
system	Use system default TCP window size for this protocol (default).
static	Manually specify TCP window size.
dynamic	Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.

tunnel-non-http	Configure how to process non-HTTP traffic when a profile configured for HTTP traffic accepts a non-HTTP session. Can occur if an application sends non-HTTP traffic using an HTTP destination port.	option	-	disable

Option	Description
enable	Pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied.
disable	Drop or tear down non-HTTP sessions accepted by the profile.

Parameter	Description	Type	Size	Default
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10
unknown-http-version	How to handle HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1.	option	-	reject

Option	Description
reject	Reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.
tunnel	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.
best-effort	Assume all HTTP sessions comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, it may not parse correctly and the connection may be lost.

config imap

Parameter	Description	Type	Size	Default
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
options	One or more options that can be applied to the session.	option	-	

Option	Description
fragmail	Pass fragmented email.
oversize	Block oversized file/email.

Parameter	Description	Type	Size	Default
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10

Parameter	Description	Type	Size	Default
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no
	Option / **Description** *no* — SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled. *yes* — SSL decryption and encryption performed by an external device.			
status	Enable/disable the active status of scanning for this protocol.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config mail-signature

Parameter	Description	Type	Size	Default
signature	Email signature to be added to outgoing email (if the signature contains spaces, enclose with quotation marks).	string	Maximum length: 1023	
status	Enable/disable adding an email signature to SMTP email messages as they pass through Container FortiOS.	option	-	disable

Option	Description
disable	Disable mail signature.
enable	Enable mail signature.

config mapi

Parameter	Description	Type	Size	Default
options	One or more options that can be applied to the session.	option	-	

Option	Description
fragmail	Pass fragmented email.
oversize	Block oversized file/email.

Parameter	Description	Type	Size	Default
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config nntp

Parameter	Description	Type	Size	Default
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
options	One or more options that can be applied to the session.	option	-	
	Option / **Description** *oversize* — Block oversized file/email. *splice* — Enable splice mode.			
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting.			

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable setting.			
status	Enable/disable the active status of scanning for this protocol. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	enable
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config pop3

Parameter	Description	Type	Size	Default
inspect-all	Enable/disable the inspection of all ports for the protocol. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	disable
options	One or more options that can be applied to the session. **Option** **Description** *fragmail* Pass fragmented email. *oversize* Block oversized file/email.	option	-	
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10

Parameter	Description	Type	Size	Default
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no

Option	Description
no	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.
yes	SSL decryption and encryption performed by an external device.

Parameter	Description	Type	Size	Default
status	Enable/disable the active status of scanning for this protocol.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config smtp

Parameter	Description	Type	Size	Default
inspect-all	Enable/disable the inspection of all ports for the protocol.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
options	One or more options that can be applied to the session.	option	-	
	Option / **Description** *fragmail* — Pass fragmented email. *oversize* — Block oversized file/email. *splice* — Enable splice mode.			
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
server-busy	Enable/disable SMTP server busy when server not available.	option	-	disable
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no

Parameter	Description	Type	Size	Default
	Option **Description** *no* SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled. *yes* SSL decryption and encryption performed by an external device.			
status	Enable/disable the active status of scanning for this protocol. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	enable
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config ssh

Parameter	Description	Type	Size	Default
comfort-amount	Amount of data to send in a transmission for client comforting.	integer	Minimum value: 1 Maximum value: 65535	1
comfort-interval	Period of time between start, or last transmission, and the next client comfort transmission of data.	integer	Minimum value: 1 Maximum value: 900	10
options	One or more options that can be applied to the session. **Option** **Description** *oversize* Block oversized file/email. *clientcomfort* Prevent client timeout. *servercomfort* Prevent server timeout.	option	-	

Parameter	Description	Type	Size	Default
oversize-limit	Maximum in-memory file size that can be scanned.	integer	Minimum value: 1 Maximum value: 799	10
scan-bzip2	Enable/disable scanning of BZip2 compressed files.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

ssl-offloaded	SSL decryption and encryption performed by an external device.	option	-	no

Option	Description
no	SSL decryption and encryption performed by Container FortiOS when deep-inspection is enabled.
yes	SSL decryption and encryption performed by an external device.

stream-based-uncompressed-limit	Maximum stream-based uncompressed data size that will be scanned.	integer	Minimum value: 0 Maximum value: 4294967295	0
tcp-window-maximum	Maximum dynamic TCP window size.	integer	Minimum value: 1048576 Maximum value: 33554432	8388608
tcp-window-minimum	Minimum dynamic TCP window size.	integer	Minimum value: 65536 Maximum value: 1048576	131072
tcp-window-size	Set TCP static window size.	integer	Minimum value: 65536 Maximum value: 33554432	262144
tcp-window-type	TCP window type to use for this protocol.	option	-	system

Parameter	Description	Type	Size	Default
	Option: *system* — Use system default TCP window size for this protocol (default). Option: *static* — Manually specify TCP window size. Option: *dynamic* — Vary TCP window size based on available memory and within limits of tcp-window-minimum and tcp-window-maximum.			
uncompressed-nest-limit	Maximum nested levels of compression that can be uncompressed and scanned.	integer	Minimum value: 2 Maximum value: 100	12
uncompressed-oversize-limit	Maximum in-memory uncompressed file size that can be scanned.	integer	Minimum value: 0 Maximum value: 799	10

config firewall schedule group

Schedule group configuration.

Syntax

```
config firewall schedule group
    edit <name>
        set member <name1>, <name2>, ...
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
member <name>	Schedules added to the schedule group. Schedule name.	string	Maximum length: 79	
name	Schedule group name.	string	Maximum length: 31	

config firewall schedule onetime

Onetime schedule configuration.

Syntax

```
config firewall schedule onetime
    edit <name>
```

```
        set end {user}
        set expiration-days {integer}
        set start {user}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
end	Schedule end date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	
expiration-days	Write an event log message this many days before the schedule expires.	integer	Minimum value: 0 Maximum value: 100	3
name	Onetime schedule name.	string	Maximum length: 31	
start	Schedule start date and time, format hh:mm yyyy/mm/dd.	user	Not Specified	

config firewall schedule recurring

Recurring schedule configuration.

Syntax

```
config firewall schedule recurring
    edit <name>
        set day {option1}, {option2}, ...
        set end {user}
        set start {user}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
day	One or more days of the week on which the schedule is valid. Separate the names of the days with a space.	option	-	none

Option	Description
sunday	Sunday.
monday	Monday.

Parameter	Description	Type	Size	Default
	Option: Description *tuesday*: Tuesday. *wednesday*: Wednesday. *thursday*: Thursday. *friday*: Friday. *saturday*: Saturday. *none*: None.			
end	Time of day to end the schedule, format hh:mm.	user	Not Specified	
name	Recurring schedule name.	string	Maximum length: 31	
start	Time of day to start the schedule, format hh:mm.	user	Not Specified	

config firewall security-policy

Configure NGFW IPv4/IPv6 application policies.

Syntax

```
config firewall security-policy
    edit <policyid>
        set action [accept|deny]
        set app-category <id1>, <id2>, ...
        set app-group <name1>, <name2>, ...
        set application <id1>, <id2>, ...
        set application-list {string}
        set av-profile {string}
        set comments {var-string}
        set custom-log-fields <field-id1>, <field-id2>, ...
        set dlp-sensor {string}
        set dnsfilter-profile {string}
        set dstaddr <name1>, <name2>, ...
        set dstaddr-negate [enable|disable]
        set dstaddr6 <name1>, <name2>, ...
        set dstintf <name1>, <name2>, ...
        set emailfilter-profile {string}
        set enforce-default-app-port [enable|disable]
        set file-filter-profile {string}
        set fsso-groups <name1>, <name2>, ...
        set groups <name1>, <name2>, ...
        set ips-sensor {string}
        set learning-mode [enable|disable]
        set logtraffic [all|utm|...]
```

```
        set name {string}
        set profile-group {string}
        set profile-protocol-options {string}
        set profile-type [single|group]
        set schedule {string}
        set send-deny-packet [disable|enable]
        set service <name1>, <name2>, ...
        set service-negate [enable|disable]
        set srcaddr <name1>, <name2>, ...
        set srcaddr-negate [enable|disable]
        set srcaddr6 <name1>, <name2>, ...
        set srcintf <name1>, <name2>, ...
        set status [enable|disable]
        set url-category <id1>, <id2>, ...
        set users <name1>, <name2>, ...
        set uuid {uuid}
        set webfilter-profile {string}
    next
end
```

config firewall security-policy

Parameter	Description	Type	Size	Default
action	Policy action (accept/deny).	option	-	deny
	Option / **Description** *accept* — Allows session that match the firewall policy. *deny* — Blocks sessions that match the firewall policy.			
app-category <id>	Application category ID list. Category IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
app-group <name>	Application group names. Application group names.	string	Maximum length: 79	
application <id>	Application ID list. Application IDs.	integer	Minimum value: 0 Maximum value: 4294967295	
application-list	Name of an existing Application list.	string	Maximum length: 35	
av-profile	Name of an existing Antivirus profile.	string	Maximum length: 35	

Parameter	Description	Type	Size	Default
comments	Comment.	var-string	Maximum length: 1023	
custom-log-fields <field-id>	Custom fields to append to log messages for this policy. Custom log field.	string	Maximum length: 35	
dlp-sensor	Name of an existing DLP sensor.	string	Maximum length: 35	
dnsfilter-profile	Name of an existing DNS filter profile.	string	Maximum length: 35	
dstaddr <name>	Destination IPv4 address name and address group names. Address name.	string	Maximum length: 79	
dstaddr-negate	When enabled dstaddr/dstaddr6 specifies what the destination address must NOT be.	option	-	disable

Option	Description
enable	Enable destination address negate.
disable	Disable destination address negate.

dstaddr6 <name>	Destination IPv6 address name and address group names. Address name.	string	Maximum length: 79	
dstintf <name>	Outgoing (egress) interface. Interface name.	string	Maximum length: 79	
emailfilter-profile	Name of an existing email filter profile.	string	Maximum length: 35	
enforce-default-app-port	Enable/disable default application port enforcement for allowed applications.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

file-filter-profile	Name of an existing file-filter profile.	string	Maximum length: 35	
fsso-groups <name>	Names of FSSO groups. Names of FSSO groups.	string	Maximum length: 511	

Parameter	Description	Type	Size	Default
groups <name>	Names of user groups that can authenticate with this policy. User group name.	string	Maximum length: 79	
ips-sensor	Name of an existing IPS sensor.	string	Maximum length: 35	
learning-mode	Enable to allow everything, but log all of the meaningful data for security information gathering. A learning report will be generated.	option	-	disable
	Option / **Description** *enable* — Enable learning mode. *disable* — Disable learning mode.			
logtraffic	Enable or disable logging. Log all sessions or security profile sessions.	option	-	utm
	Option / **Description** *all* — Log all sessions accepted or denied by this policy. *utm* — Log traffic that has a security profile applied to it. *disable* — Disable all logging for this policy.			
name	Policy name.	string	Maximum length: 35	
policyid	Policy ID.	integer	Minimum value: 0 Maximum value: 4294967294	0
profile-group	Name of profile group.	string	Maximum length: 35	
profile-protocol-options	Name of an existing Protocol options profile.	string	Maximum length: 35	default
profile-type	Determine whether the firewall policy allows security profile groups or single profiles only.	option	-	single
	Option / **Description** *single* — Do not allow security profile groups. *group* — Allow security profile groups.			

Parameter	Description	Type	Size	Default
schedule	Schedule name.	string	Maximum length: 35	
send-deny-packet	Enable to send a reply when a session is denied or blocked by a firewall policy.	option	-	disable

Option	Description
disable	Disable deny-packet sending.
enable	Enable deny-packet sending.

Parameter	Description	Type	Size	Default
service <name>	Service and service group names. Service name.	string	Maximum length: 79	
service-negate	When enabled service specifies what the service must NOT be.	option	-	disable

Option	Description
enable	Enable negated service match.
disable	Disable negated service match.

Parameter	Description	Type	Size	Default
srcaddr <name>	Source IPv4 address name and address group names. Address name.	string	Maximum length: 79	
srcaddr-negate	When enabled srcaddr/srcaddr6 specifies what the source address must NOT be.	option	-	disable

Option	Description
enable	Enable source address negate.
disable	Disable source address negate.

Parameter	Description	Type	Size	Default
srcaddr6 <name>	Source IPv6 address name and address group names. Address name.	string	Maximum length: 79	
srcintf <name>	Incoming (ingress) interface. Interface name.	string	Maximum length: 79	
status	Enable or disable this policy.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
url-category <id>	URL category ID list. URL category ID.	integer	Minimum value: 0 Maximum value: 255	
users <name>	Names of individual users that can authenticate with this policy. User name.	string	Maximum length: 79	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000
webfilter-profile	Name of an existing Web filter profile.	string	Maximum length: 35	

config firewall service category

Configure service categories.

Syntax

```
config firewall service category
    edit <name>
        set comment {var-string}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Service category name.	string	Maximum length: 63	

config firewall service custom

Configure custom services.

Syntax

```
config firewall service custom
    edit <name>
        set category {string}
        set check-reset-range [disable|strict|...]
        set comment {var-string}
```

```
        set fqdn {string}
        set icmpcode {integer}
        set icmptype {integer}
        set iprange {user}
        set protocol [TCP/UDP/SCTP|ICMP|...]
        set protocol-number {integer}
        set sctp-portrange {user}
        set session-ttl {user}
        set tcp-halfclose-timer {integer}
        set tcp-halfopen-timer {integer}
        set tcp-portrange {user}
        set tcp-rst-timer {integer}
        set tcp-timewait-timer {integer}
        set udp-idle-timer {integer}
        set udp-portrange {user}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
category	Service category.	string	Maximum length: 63	
check-reset-range	Configure the type of ICMP error message verification.	option	-	default
	Option / **Description** *disable* — Disable RST range check. *strict* — Check RST range strictly. *default* — Using system default setting.			
comment	Comment.	var-string	Maximum length: 255	
fqdn	Fully qualified domain name.	string	Maximum length: 255	
icmpcode	ICMP code.	integer	Minimum value: 0 Maximum value: 255	
icmptype	ICMP type, value from 0 to 255	integer	Minimum value: 0 Maximum value: 255	
iprange	Start and end of the IP range associated with service.	user	Not Specified	

Parameter	Description	Type	Size	Default
name	Custom service name.	string	Maximum length: 79	
protocol	Protocol type based on IANA numbers.	option	-	TCP/UDP/SCTP

Option	Description
TCP/UDP/SCTP	TCP, UDP and SCTP.
ICMP	ICMP.
ICMP6	ICMP6.
IP	IP.

protocol-number	IP protocol number.	integer	Minimum value: 0 Maximum value: 254	0
sctp-portrange	Multiple SCTP port ranges.	user	Not Specified	
session-ttl	Session TTL.	user	Not Specified	
tcp-halfclose-timer	Wait time to close a TCP session waiting for an unanswered FIN packet.	integer	Minimum value: 0 Maximum value: 86400	0
tcp-halfopen-timer	Wait time to close a TCP session waiting for an unanswered open session packet.	integer	Minimum value: 0 Maximum value: 86400	0
tcp-portrange	Multiple TCP port ranges.	user	Not Specified	
tcp-rst-timer	Set the length of the TCP CLOSE state in seconds.	integer	Minimum value: 5 Maximum value: 300	0
tcp-timewait-timer	Set the length of the TCP TIME-WAIT state in seconds.	integer	Minimum value: 0 Maximum value: 300	0

Parameter	Description	Type	Size	Default
udp-idle-timer	UDP half close timeout.	integer	Minimum value: 0 Maximum value: 86400	0
udp-portrange	Multiple UDP port ranges.	user	Not Specified	

config firewall service group

Configure service groups.

Syntax

```
config firewall service group
    edit <name>
        set comment {var-string}
        set member <name1>, <name2>, ...
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
member <name>	Service objects contained within the group. Address name.	string	Maximum length: 79	
name	Address group name.	string	Maximum length: 79	

config firewall ssl-ssh-profile

Configure SSL/SSH protocol options.

Syntax

```
config firewall ssl-ssh-profile
    edit <name>
        set block-blocklisted-certificates [disable|enable]
        set caname {string}
        set comment {var-string}
        config dot
            Description: Configure DNS over TLS options.
            set cert-validation-failure [allow|block|...]
```

```
        set cert-validation-timeout [allow|block|...]
        set client-certificate [bypass|inspect|...]
        set expired-server-cert [allow|block|...]
        set proxy-after-tcp-handshake [enable|disable]
        set revoked-server-cert [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set status [disable|deep-inspection]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set untrusted-server-cert [allow|block|...]
    end
    config ftps
        Description: Configure FTPS options.
        set cert-validation-failure [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set client-certificate [bypass|inspect|...]
        set expired-server-cert [allow|block|...]
        set revoked-server-cert [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set status [disable|deep-inspection]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set untrusted-server-cert [allow|block|...]
    end
    config https
        Description: Configure HTTPS options.
        set cert-probe-failure [allow|block]
        set cert-validation-failure [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set client-certificate [bypass|inspect|...]
        set expired-server-cert [allow|block|...]
        set proxy-after-tcp-handshake [enable|disable]
        set revoked-server-cert [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set status [disable|certificate-inspection|...]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set untrusted-server-cert [allow|block|...]
    end
    config imaps
        Description: Configure IMAPS options.
        set cert-validation-failure [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set client-certificate [bypass|inspect|...]
        set expired-server-cert [allow|block|...]
        set proxy-after-tcp-handshake [enable|disable]
        set revoked-server-cert [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set status [disable|deep-inspection]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set untrusted-server-cert [allow|block|...]
    end
    set mapi-over-https [enable|disable]
    config pop3s
        Description: Configure POP3S options.
```

```
        set cert-validation-failure [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set client-certificate [bypass|inspect|...]
        set expired-server-cert [allow|block|...]
        set proxy-after-tcp-handshake [enable|disable]
        set revoked-server-cert [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set status [disable|deep-inspection]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set untrusted-server-cert [allow|block|...]
    end
    set rpc-over-https [enable|disable]
    set server-cert <name1>, <name2>, ...
    set server-cert-mode [re-sign|replace]
    config smtps
        Description: Configure SMTPS options.
        set cert-validation-failure [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set client-certificate [bypass|inspect|...]
        set expired-server-cert [allow|block|...]
        set proxy-after-tcp-handshake [enable|disable]
        set revoked-server-cert [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set status [disable|deep-inspection]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set untrusted-server-cert [allow|block|...]
    end
    config ssh
        Description: Configure SSH options.
        set inspect-all [disable|deep-inspection]
        set proxy-after-tcp-handshake [enable|disable]
        set ssh-algorithm [compatible|high-encryption]
        set ssh-tun-policy-check [disable|enable]
        set status [disable|deep-inspection]
        set unsupported-version [bypass|block]
    end
    config ssl
        Description: Configure SSL options.
        set cert-validation-failure [allow|block|...]
        set cert-validation-timeout [allow|block|...]
        set client-certificate [bypass|inspect|...]
        set expired-server-cert [allow|block|...]
        set inspect-all [disable|certificate-inspection|...]
        set revoked-server-cert [allow|block|...]
        set sni-server-cert-check [enable|strict|...]
        set unsupported-ssl-cipher [allow|block]
        set unsupported-ssl-negotiation [allow|block]
        set untrusted-server-cert [allow|block|...]
    end
    set ssl-anomalies-log [disable|enable]
    config ssl-exempt
        Description: Servers to exempt from SSL inspection.
        edit <id>
            set address {string}
```

```
                set address6 {string}
                set fortiguard-category {integer}
                set regex {string}
                set type [fortiguard-category|address|...]
                set wildcard-fqdn {string}
            next
        end
        set ssl-exemptions-log [disable|enable]
        set ssl-negotiation-log [disable|enable]
        config ssl-server
            Description: SSL server settings used for client certificate request.
            edit <id>
                set ftps-client-certificate [bypass|inspect|...]
                set https-client-certificate [bypass|inspect|...]
                set imaps-client-certificate [bypass|inspect|...]
                set ip {ipv4-address-any}
                set pop3s-client-certificate [bypass|inspect|...]
                set smtps-client-certificate [bypass|inspect|...]
                set ssl-other-client-certificate [bypass|inspect|...]
            next
        end
        set supported-alpn [http1-1|http2|...]
        set untrusted-caname {string}
        set use-ssl-server [disable|enable]
    next
end
```

config firewall ssl-ssh-profile

Parameter	Description	Type	Size	Default
block-blocklisted-certificates	Enable/disable blocking SSL-based botnet communication by FortiGuard certificate blocklist.	option	-	enable

Option	Description
disable	Disable FortiGuard certificate blocklist.
enable	Enable FortiGuard certificate blocklist.

caname	CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_SSL
comment	Optional comments.	var-string	Maximum length: 255	
mapi-over-https	Enable/disable inspection of MAPI over HTTPS.	option	-	disable

Option	Description
enable	Enable inspection of MAPI over HTTPS.
disable	Disable inspection of MAPI over HTTPS.

Parameter	Description	Type	Size	Default
name	Name.	string	Maximum length: 35	
rpc-over-https	Enable/disable inspection of RPC over HTTPS.	option	-	disable

Option	Description
enable	Enable inspection of RPC over HTTPS.
disable	Disable inspection of RPC over HTTPS.

server-cert <name>	Certificate used by SSL Inspection to replace server certificate. Certificate list.	string	Maximum length: 35	
server-cert-mode	Re-sign or replace the server's certificate.	option	-	re-sign

Option	Description
re-sign	Multiple clients connecting to multiple servers.
replace	Protect an SSL server.

ssl-anomalies-log	Enable/disable logging SSL anomalies.	option	-	enable

Option	Description
disable	Disable logging SSL anomalies.
enable	Enable logging SSL anomalies.

ssl-exemptions-log	Enable/disable logging SSL exemptions.	option	-	disable

Option	Description
disable	Disable logging SSL exemptions.
enable	Enable logging SSL exemptions.

ssl-negotiation-log	Enable/disable logging SSL negotiation.	option	-	disable

Option	Description
disable	Disable logging SSL negotiation.
enable	Enable logging SSL negotiation.

Parameter	Description	Type	Size	Default
supported-alpn	Configure ALPN option.	option	-	all

Option	Description
http1-1	Enable ALPN of HTTP1.1.
http2	Enable ALPN of HTTP2.
all	Enable ALPN of HTTP1.1 and HTTP2.
none	Do not use ALPN.

untrusted-caname	Untrusted CA certificate used by SSL Inspection.	string	Maximum length: 35	Fortinet_CA_Untrusted
use-ssl-server	Enable/disable the use of SSL server table for SSL offloading.	option	-	disable

Option	Description
disable	Don't use SSL server configuration.
enable	Use SSL server configuration.

config dot

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

client-certificate	Action based on received client certificate.	option	-	bypass

Parameter	Description	Type	Size	Default
	Option / **Description** *bypass* / Bypass the session. *inspect* / Inspect the session. *block* / Block the session.			
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option / **Description** *allow* / Allow the server certificate. *block* / Block the session. *ignore* / Re-sign the server certificate as trusted.			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option / **Description** *allow* / Allow the server certificate. *block* / Block the session. *ignore* / Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option / **Description** *enable* / Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* / Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* / Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			

Parameter	Description	Type	Size	Default
status	Configure protocol inspection status.	option	-	disable

Option	Description
disable	Disable.
deep-inspection	Full SSL inspection.

Parameter	Description	Type	Size	Default
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow

Option	Description
allow	Bypass the session when the cipher is not supported.
block	Block the session when the cipher is not supported.

Parameter	Description	Type	Size	Default
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow

Option	Description
allow	Bypass the session when the negotiation is not supported.
block	Block the session when the negotiation is not supported.

Parameter	Description	Type	Size	Default
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

config ftps

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
client-certificate	Action based on received client certificate.	option	-	bypass

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size	Default
expired-server-cert	Action based on server certificate is expired.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
revoked-server-cert	Action based on server certificate is revoked.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable

Option	Description
enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.
strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
status	Configure protocol inspection status.	option	-	deep-inspection
	Option **Description** *disable* Disable. *deep-inspection* Full SSL inspection.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option **Description** *allow* Bypass the session when the cipher is not supported. *block* Block the session when the cipher is not supported.			
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option **Description** *allow* Bypass the session when the negotiation is not supported. *block* Block the session when the negotiation is not supported.			
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			

config https

Parameter	Description	Type	Size	Default
cert-probe-failure	Action based on certificate probe failure.	option	-	block

Parameter	Description	Type	Size	Default
	Option / **Description** *allow* — Bypass the session when unable to retrieve server's certificate for inspection. *block* — Block the session when unable to retrieve server's certificate for inspection.			
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
client-certificate	Action based on received client certificate.	option	-	bypass
	Option / **Description** *bypass* — Bypass the session. *inspect* — Inspect the session. *block* — Block the session.			
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable setting. *disable* — Disable setting.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
status	Configure protocol inspection status.	option	-	deep-inspection
	Option / **Description** *disable* — Disable. *certificate-inspection* — Inspect SSL handshake only. *deep-inspection* — Full SSL inspection.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the cipher is not supported. *block* — Block the session when the cipher is not supported.			

Parameter	Description	Type	Size	Default
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow

Option	Description
allow	Bypass the session when the negotiation is not supported.
block	Block the session when the negotiation is not supported.

Parameter	Description	Type	Size	Default
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

config imaps

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
client-certificate	Action based on received client certificate.	option	-	inspect

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.

Parameter	Description	Type	Size	Default
	Option **Description** *block* Block the session.			
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option **Description** *enable* Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
status	Configure protocol inspection status.	option	-	deep-inspection

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable. *deep-inspection* Full SSL inspection.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option **Description** *allow* Bypass the session when the cipher is not supported. *block* Block the session when the cipher is not supported.			
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option **Description** *allow* Bypass the session when the negotiation is not supported. *block* Block the session when the negotiation is not supported.			
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			

config pop3s

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Parameter	Description	Type	Size	Default
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			
client-certificate	Action based on received client certificate.	option	-	inspect
	Option **Description** *bypass* Bypass the session. *inspect* Inspect the session. *block* Block the session.			
expired-server-cert	Action based on server certificate is expired.	option	-	block
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
status	Configure protocol inspection status.	option	-	deep-inspection
	Option / **Description** *disable* — Disable. *deep-inspection* — Full SSL inspection.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the cipher is not supported. *block* — Block the session when the cipher is not supported.			
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the negotiation is not supported. *block* — Block the session when the negotiation is not supported.			
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			

config smtps

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
client-certificate	Action based on received client certificate.	option	-	inspect

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size	Default
expired-server-cert	Action based on server certificate is expired.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
revoked-server-cert	Action based on server certificate is revoked.	option	-	block

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

Parameter	Description	Type	Size	Default
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable

Option	Description
enable	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.
strict	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.
disable	Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.

Parameter	Description	Type	Size	Default
status	Configure protocol inspection status.	option	-	deep-inspection

Option	Description
disable	Disable.
deep-inspection	Full SSL inspection.

Parameter	Description	Type	Size	Default
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow

Option	Description
allow	Bypass the session when the cipher is not supported.
block	Block the session when the cipher is not supported.

Parameter	Description	Type	Size	Default
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow

Option	Description
allow	Bypass the session when the negotiation is not supported.
block	Block the session when the negotiation is not supported.

Parameter	Description	Type	Size	Default
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

config ssh

Parameter	Description	Type	Size	Default
inspect-all	Level of SSL inspection.	option	-	disable

Option	Description
disable	Disable.
deep-inspection	Full SSL inspection.

Parameter	Description	Type	Size	Default
proxy-after-tcp-handshake	Proxy traffic after the TCP 3-way handshake has been established (not before).	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
ssh-algorithm	Relative strength of encryption algorithms accepted during negotiation.	option	-	compatible

Option	Description
compatible	Allow a broader set of encryption algorithms for best compatibility.
high-encryption	Allow only AES-CTR, AES-GCM ciphers and high encryption algorithms.

Parameter	Description	Type	Size	Default
ssh-tun-policy-check	Enable/disable SSH tunnel policy check.	option	-	disable

Option	Description
disable	Disable SSH tunnel policy check.
enable	Enable SSH tunnel policy check.

Parameter	Description	Type	Size	Default
status	Configure protocol inspection status.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *disable* Disable. *deep-inspection* Full SSL inspection.			
unsupported-version	Action based on SSH version being unsupported.	option	-	bypass
	Option **Description** *bypass* Bypass the session. *block* Block the session.			

config ssl

Parameter	Description	Type	Size	Default
cert-validation-failure	Action based on certificate validation failure.	option	-	block
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			
cert-validation-timeout	Action based on certificate validation timeout.	option	-	allow
	Option **Description** *allow* Allow the server certificate. *block* Block the session. *ignore* Re-sign the server certificate as trusted.			
client-certificate	Action based on received client certificate.	option	-	bypass
	Option **Description** *bypass* Bypass the session. *inspect* Inspect the session. *block* Block the session.			
expired-server-cert	Action based on server certificate is expired.	option	-	block

Parameter	Description	Type	Size	Default
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
inspect-all	Level of SSL inspection.	option	-	disable
	Option / **Description** *disable* — Disable. *certificate-inspection* — Inspect SSL handshake only. *deep-inspection* — Full SSL inspection.			
revoked-server-cert	Action based on server certificate is revoked.	option	-	block
	Option / **Description** *allow* — Allow the server certificate. *block* — Block the session. *ignore* — Re-sign the server certificate as trusted.			
sni-server-cert-check	Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.	option	-	enable
	Option / **Description** *enable* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering. *strict* — Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection. *disable* — Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.			
unsupported-ssl-cipher	Action based on the SSL cipher used being unsupported.	option	-	allow
	Option / **Description** *allow* — Bypass the session when the cipher is not supported. *block* — Block the session when the cipher is not supported.			

Parameter	Description	Type	Size	Default
unsupported-ssl-negotiation	Action based on the SSL negotiation used being unsupported.	option	-	allow

Option	Description
allow	Bypass the session when the negotiation is not supported.
block	Block the session when the negotiation is not supported.

Parameter	Description	Type	Size	Default
untrusted-server-cert	Action based on server certificate is not issued by a trusted CA.	option	-	allow

Option	Description
allow	Allow the server certificate.
block	Block the session.
ignore	Re-sign the server certificate as trusted.

config ssl-exempt

Parameter	Description	Type	Size	Default
address	IPv4 address object.	string	Maximum length: 79	
address6	IPv6 address object.	string	Maximum length: 79	
fortiguard-category	FortiGuard category ID.	integer	Minimum value: 0 Maximum value: 255	0
id	ID number.	integer	Minimum value: 0 Maximum value: 512	0
regex	Exempt servers by regular expression.	string	Maximum length: 255	
type	Type of address object (IPv4 or IPv6) or FortiGuard category.	option	-	fortiguard-category

Option	Description
fortiguard-category	FortiGuard category.
address	Firewall IPv4 address.

Parameter	Description	Type	Size	Default
	Option **Description** *address6* Firewall IPv6 address. *wildcard-fqdn* Fully Qualified Domain Name with wildcard characters. *regex* Regular expression FQDN.			
wildcard-fqdn	Exempt servers by wildcard FQDN.	string	Maximum length: 79	

config ssl-server

Parameter	Description	Type	Size	Default
ftps-client-certificate	Action based on received client certificate during the FTPS handshake.	option	-	bypass
	Option **Description** *bypass* Bypass the session. *inspect* Inspect the session. *block* Block the session.			
https-client-certificate	Action based on received client certificate during the HTTPS handshake.	option	-	bypass
	Option **Description** *bypass* Bypass the session. *inspect* Inspect the session. *block* Block the session.			
id	SSL server ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
imaps-client-certificate	Action based on received client certificate during the IMAPS handshake.	option	-	bypass
	Option **Description** *bypass* Bypass the session. *inspect* Inspect the session. *block* Block the session.			

Parameter	Description	Type	Size	Default
ip	IPv4 address of the SSL server.	ipv4-address-any	Not Specified	0.0.0.0
pop3s-client-certificate	Action based on received client certificate during the POP3S handshake.	option	-	bypass

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size	Default
smtps-client-certificate	Action based on received client certificate during the SMTPS handshake.	option	-	bypass

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

Parameter	Description	Type	Size	Default
ssl-other-client-certificate	Action based on received client certificate during an SSL protocol handshake.	option	-	bypass

Option	Description
bypass	Bypass the session.
inspect	Inspect the session.
block	Block the session.

config firewall vip

Configure virtual IP for IPv4.

Syntax

```
config firewall vip
    edit <name>
        set comment {var-string}
        set extintf {string}
        set extip {user}
        set extport {user}
        set id {integer}
        set mappedip <range1>, <range2>, ...
        set mappedport {user}
```

```
        set portforward [disable|enable]
        set portmapping-type [1-to-1|m-to-n]
        set protocol [tcp|udp|...]
        set service <name1>, <name2>, ...
        set type [static-nat|access-proxy]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
extintf	Interface connected to the source network that receives the packets that will be forwarded to the destination network.	string	Maximum length: 35	
extip	IP address or address range on the external interface that you want to map to an address or address range on the destination network.	user	Not Specified	
extport	Incoming port number range that you want to map to a port number range on the destination network.	user	Not Specified	
id	Custom defined ID.	integer	Minimum value: 0 Maximum value: 65535	0
mappedip <range>	IP address or address range on the destination network to which the external IP address is mapped. Mapped IP range.	string	Maximum length: 79	
mappedport	Port number range on the destination network to which the external port number range is mapped.	user	Not Specified	
name	Virtual IP name.	string	Maximum length: 79	
portforward	Enable/disable port forwarding.	option	-	disable

Option	Description
disable	Disable port forward.
enable	Enable port forward.

portmapping-type	Port mapping type.	option	-	1-to-1

Parameter	Description	Type	Size	Default
	Option **Description** *1-to-1* One to one. *m-to-n* Many to many.			
protocol	Protocol to use when forwarding packets.	option	-	tcp
	Option **Description** *tcp* TCP. *udp* UDP. *sctp* SCTP. *icmp* ICMP.			
service <name>	Service name. Service name.	string	Maximum length: 79	
type	Configure a static NAT or access proxy.	option	-	static-nat
	Option **Description** *static-nat* Static NAT. *access-proxy* Access proxy.			

config firewall wildcard-fqdn custom

Config Wildcard FQDN address.

Syntax

```
config firewall wildcard-fqdn custom
    edit <name>
        set comment {var-string}
        set wildcard-fqdn {string}
    next
end
```

config firewall wildcard-fqdn custom

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
name	Address name.	string	Maximum length: 79	

Parameter	Description	Type	Size	Default
wildcard-fqdn	Wildcard FQDN.	string	Maximum length: 255	

ips

This section includes syntax for the following commands:

- config ips global on page 110
- config ips rule on page 113
- config ips sensor on page 115
- config ips settings on page 120

config ips global

Configure IPS global parameter.

Syntax

```
config ips global
    set anomaly-mode [periodical|continuous]
    set database [regular|extended]
    set deep-app-insp-db-limit {integer}
    set deep-app-insp-timeout {integer}
    set engine-count {integer}
    set exclude-signatures [none|industrial]
    set fail-open [enable|disable]
    set ngfw-max-scan-range {integer}
    set packet-log-queue-depth {integer}
    set session-limit-mode [accurate|heuristic]
    set socket-size {integer}
    set sync-session-ttl [enable|disable]
    config tls-active-probe
        Description: TLS active probe configuration.
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set source-ip {ipv4-address}
        set source-ip6 {ipv6-address}
    end
    set traffic-submit [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
anomaly-mode	Global blocking mode for rate-based anomalies.	option	-	continuous

Parameter	Description	Type	Size	Default
	Option / **Description** *periodical* — After an anomaly is detected, allow the number of packets per second according to the anomaly configuration. *continuous* — Block packets once an anomaly is detected. Overrides individual anomaly settings.			
database	Regular or extended IPS database. Regular protects against the latest common and in-the-wild attacks. Extended includes protection from legacy attacks.	option	-	regular
	Option / **Description** *regular* — IPS regular database package. *extended* — IPS extended database package.			
deep-app-insp-db-limit	Limit on number of entries in deep application inspection database	integer	Minimum value: 0 Maximum value: 2147483647	0
deep-app-insp-timeout	Timeout for Deep application inspection.	integer	Minimum value: 0 Maximum value: 2147483647	0
engine-count	Number of IPS engines running. If set to the default value of 0, FortiOS sets the number to optimize performance depending on the number of CPU cores.	integer	Minimum value: 0 Maximum value: 255	0
exclude-signatures	Excluded signatures.	option	-	industrial
	Option / **Description** *none* — No signatures excluded. *industrial* — Exclude industrial signatures.			
fail-open	Enable to allow traffic if the IPS process crashes. Default is disable and IPS traffic is blocked when the IPS process crashes.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* — Enable IPS fail open. *disable* — Disable IPS fail open.			
ngfw-max-scan-range	NGFW policy-mode app detection threshold.	integer	Minimum value: 0 Maximum value: 4294967295	4096
packet-log-queue-depth	Packet/pcap log queue depth per IPS engine.	integer	Minimum value: 128 Maximum value: 4096	128
session-limit-mode	Method of counting concurrent sessions used by session limit anomalies. Choose between greater accuracy (accurate) or improved performance (heuristics).	option	-	heuristic
	Option / **Description** *accurate* — Accurately count concurrent sessions, demands more resources. *heuristic* — Use heuristics to estimate the number of concurrent sessions. Acceptable in most cases.			
socket-size	IPS socket buffer size. Max and default value depend on available memory. Can be changed to tune performance.	integer	Minimum value: 0 Maximum value: 512	256
sync-session-ttl	Enable/disable use of kernel session TTL for IPS sessions.	option	-	enable
	Option / **Description** *enable* — Enable use of kernel session TTL for IPS sessions. *disable* — Disable use of kernel session TTL for IPS sessions.			
traffic-submit	Enable/disable submitting attack data found by this Container FortiOS to FortiGuard.	option	-	disable
	Option / **Description** *enable* — Enable traffic submit. *disable* — Disable traffic submit.			

config tls-active-probe

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

Parameter	Description	Type	Size	Default
source-ip	Source IP address used for TLS active probe.	ipv4-address	Not Specified	0.0.0.0
source-ip6	Source IPv6 address used for TLS active probe.	ipv6-address	Not Specified	::

config ips rule

Configure IPS rules. Read-only.

This table cannot be edited.

Syntax

```
config ips rule
    edit <name>
        get
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
action	Action.	option	-	pass

Option	Description
pass	Pass or allow matching traffic.
block	Block or drop matching traffic.

Parameter	Description	Type	Size	Default
application	Vulnerable applications.	user	Not Specified	

Parameter	Description	Type	Size	Default
date	Date.	integer	Minimum value: 0 Maximum value: 4294967295	0
group	Group.	string	Maximum length: 63	
location	Vulnerable location.	user	Not Specified	
log	Enable/disable logging.	option	-	enable

Option	Description
disable	Disable logging.
enable	Enable logging.

log-packet	Enable/disable packet logging.	option	-	disable

Option	Description
disable	Disable packet logging.
enable	Enable packet logging.

name	Rule name.	string	Maximum length: 63	
os	Vulnerable operation systems.	user	Not Specified	
rev	Revision.	integer	Minimum value: 0 Maximum value: 4294967295	0
rule-id	Rule ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
service	Vulnerable service.	user	Not Specified	
severity	Severity.	user	Not Specified	
status	Enable/disable status.	option	-	enable

Option	Description
disable	Disable status.
enable	Enable status.

config ips sensor

Configure IPS sensor.

Syntax

```
config ips sensor
    edit <name>
        set block-malicious-url [disable|enable]
        set comment {var-string}
        config entries
            Description: IPS sensor filter.
            edit <id>
                set action [pass|block|...]
                set application {user}
                set cve <cve-entry1>, <cve-entry2>, ...
                config exempt-ip
                    Description: Traffic from selected source or destination IP addresses is
exempt from this signature.
                    edit <id>
                        set dst-ip {ipv4-classnet}
                        set src-ip {ipv4-classnet}
                    next
                end
                set location {user}
                set log [disable|enable]
                set log-attack-context [disable|enable]
                set log-packet [disable|enable]
                set os {user}
                set protocol {user}
                set quarantine [none|attacker]
                set quarantine-expiry {user}
                set quarantine-log [disable|enable]
                set rate-count {integer}
                set rate-duration {integer}
                set rate-mode [periodical|continuous]
                set rate-track [none|src-ip|...]
                set rule <id1>, <id2>, ...
                set severity {user}
                set status [disable|enable|...]
            next
        end
        set extended-log [enable|disable]
        set replacemsg-group {string}
        set scan-botnet-connections [disable|block|...]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
block-malicious-url	Enable/disable malicious URL blocking.	option	-	disable

Option	Description
disable	Disable malicious URL blocking.
enable	Enable malicious URL blocking.

comment	Comment.	var-string	Maximum length: 255	
extended-log	Enable/disable extended logging.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

name	Sensor name.	string	Maximum length: 35	
replacemsg-group	Replacement message group.	string	Maximum length: 35	
scan-botnet-connections	Block or monitor connections to Botnet servers, or disable Botnet scanning.	option	-	disable

Option	Description
disable	Do not scan connections to botnet servers.
block	Block connections to botnet servers.
monitor	Log connections to botnet servers.

config entries

Parameter	Description	Type	Size	Default
action	Action taken with traffic in which signatures are detected.	option	-	default

Option	Description
pass	Pass or allow matching traffic.
block	Block or drop matching traffic.

Parameter	Description	Type	Size	Default
	Option / **Description** *reset* — Reset sessions for matching traffic. *default* — Pass or drop matching traffic, depending on the default action of the signature.			
application	Applications to be protected. set application ? lists available applications. all includes all applications. other includes all unlisted applications.	user	Not Specified	all
cve <cve-entry>	List of CVE IDs of the signatures to add to the sensor CVE IDs or CVE wildcards.	string	Maximum length: 19	
id	Rule ID in IPS database.	integer	Minimum value: 0 Maximum value: 4294967295	0
location	Protect client or server traffic.	user	Not Specified	all
log	Enable/disable logging of signatures included in filter.	option	-	enable
	Option / **Description** *disable* — Disable logging of selected rules. *enable* — Enable logging of selected rules.			
log-attack-context	Enable/disable logging of attack context: URL buffer, header buffer, body buffer, packet buffer.	option	-	disable
	Option / **Description** *disable* — Disable logging of detailed attack context. *enable* — Enable logging of detailed attack context.			
log-packet	Enable/disable packet logging. Enable to save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use.	option	-	disable
	Option / **Description** *disable* — Disable packet logging of selected rules. *enable* — Enable packet logging of selected rules.			

Parameter	Description	Type	Size	Default
os	Operating systems to be protected. all includes all operating systems. other includes all unlisted operating systems.	user	Not Specified	all
protocol	Protocols to be examined. set protocol ? lists available protocols. all includes all protocols. other includes all unlisted protocols.	user	Not Specified	all
quarantine	Quarantine method.	option	-	none
	Option / **Description** *none* — Quarantine is disabled. *attacker* — Block all traffic sent from attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected.			
quarantine-expiry	Duration of quarantine. Requires quarantine set to attacker.	user	Not Specified	5m
quarantine-log	Enable/disable quarantine logging.	option	-	enable
	Option / **Description** *disable* — Disable quarantine logging. *enable* — Enable quarantine logging.			
rate-count	Count of the rate.	integer	Minimum value: 0 Maximum value: 65535	0
rate-duration	Duration (sec) of the rate.	integer	Minimum value: 1 Maximum value: 65535	60
rate-mode	Rate limit mode.	option	-	continuous
	Option / **Description** *periodical* — Allow configured number of packets every rate-duration. *continuous* — Block packets once the rate is reached.			
rate-track	Track the packet protocol field.	option	-	none
	Option / **Description** *none* — none			

Parameter	Description	Type	Size	Default
	Option / **Description** *src-ip* / Source IP. *dest-ip* / Destination IP. *dhcp-client-mac* / DHCP client. *dns-domain* / DNS domain.			
rule <id>	Identifies the predefined or custom IPS signatures to add to the sensor. Rule IPS.	integer	Minimum value: 0 Maximum value: 4294967295	
severity	Relative severity of the signature, from info to critical. Log messages generated by the signature include the severity.	user	Not Specified	all
status	Status of the signatures included in filter. default enables the filter and only use filters with default status of enable. Filters with default status of disable will not be used.	option	-	default
	Option / **Description** *disable* / Disable status of selected rules. *enable* / Enable status of selected rules. *default* / Default.			

config exempt-ip

Parameter	Description	Type	Size	Default
dst-ip	Destination IP address and netmask.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
id	Exempt IP ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
src-ip	Source IP address and netmask.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0

config ips settings

Configure IPS parameter.

Syntax

```
config ips settings
    set ips-packet-quota {integer}
    set packet-log-history {integer}
    set packet-log-memory {integer}
    set packet-log-post-attack {integer}
end
```

Parameters

Parameter	Description	Type	Size	Default
ips-packet-quota	Maximum amount of disk space in MB for logged packets when logging to disk. Range depends on disk size.	integer	Minimum value: 0 Maximum value: 4294967295	0
packet-log-history	Number of packets to capture before and including the one in which the IPS signature is detected.	integer	Minimum value: 1 Maximum value: 255	1
packet-log-memory	Maximum memory can be used by packet log.	integer	Minimum value: 64 Maximum value: 8192	256
packet-log-post-attack	Number of packets to log after the IPS signature is detected.	integer	Minimum value: 0 Maximum value: 255	0

log

This section includes syntax for the following commands:

- config log custom-field on page 121
- config log disk setting on page 121
- config log memory global-setting on page 127
- config log memory setting on page 128
- config log setting on page 128
- config log syslogd2 filter on page 130
- config log syslogd2 setting on page 132
- config log syslogd3 filter on page 136
- config log syslogd3 setting on page 138
- config log syslogd4 filter on page 141
- config log syslogd4 setting on page 143
- config log syslogd filter on page 147
- config log syslogd setting on page 149

config log custom-field

Configure custom log fields.

Syntax

```
config log custom-field
    edit <id>
        set name {string}
        set value {string}
    next
end
```

config log custom-field

Parameter	Description	Type	Size	Default
id	field ID <string>.	string	Maximum length: 35	
name	Field name (max: 15 characters).	string	Maximum length: 15	
value	Field value (max: 63 characters).	string	Maximum length: 63	

config log disk setting

Settings for local disk logging.

Syntax

```
config log disk setting
    set diskfull [overwrite|nolog]
    set dlp-archive-quota {integer}
    set full-final-warning-threshold {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set ips-archive [enable|disable]
    set log-quota {integer}
    set max-log-file-size {integer}
    set max-policy-packet-capture-size {integer}
    set maximum-log-age {integer}
    set report-quota {integer}
    set roll-day {option1}, {option2}, ...
    set roll-schedule [daily|weekly]
    set roll-time {user}
    set source-ip {ipv4-address}
    set status [enable|disable]
    set upload [enable|disable]
    set upload-delete-files [enable|disable]
    set upload-destination {option}
    set upload-ssl-conn [default|high|...]
    set uploaddir {string}
    set uploadip {ipv4-address}
    set uploadpass {password}
    set uploadport {integer}
    set uploadsched [disable|enable]
    set uploadtime {user}
    set uploadtype {option1}, {option2}, ...
    set uploaduser {string}
end
```

Parameters

Parameter	Description	Type	Size	Default
diskfull	Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full.	option	-	overwrite
	Option / **Description** *overwrite* — Overwrite the oldest logs when the log disk is full. *nolog* — Stop logging when the log disk is full.			
dlp-archive-quota	DLP archive quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
full-final-warning-threshold	Log full final warning threshold as a percent.	integer	Minimum value: 3 Maximum value: 100	95
full-first-warning-threshold	Log full first warning threshold as a percent.	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent.	integer	Minimum value: 2 Maximum value: 99	90
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

ips-archive	Enable/disable IPS packet archiving to the local disk.	option	-	enable

Option	Description
enable	Enable IPS packet archiving.
disable	Disable IPS packet archiving.

log-quota	Disk log quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
max-log-file-size	Maximum log file size before rolling.	integer	Minimum value: 1 Maximum value: 100	20

Parameter	Description	Type	Size	Default
max-policy-packet-capture-size	Maximum size of policy sniffer in MB (0 means unlimited).	integer	Minimum value: 0 Maximum value: 4294967295	100
maximum-log-age	Delete log files older than (days).	integer	Minimum value: 0 Maximum value: 3650	7
report-quota	Report quota (MB).	integer	Minimum value: 0 Maximum value: 4294967295	0
roll-day	Day of week on which to roll log file.	option	-	sunday

Option	Description
sunday	Sunday
monday	Monday
tuesday	Tuesday
wednesday	Wednesday
thursday	Thursday
friday	Friday
saturday	Saturday

roll-schedule	Frequency to check log file for rolling.	option	-	daily

Option	Description
daily	Check the log file once a day.
weekly	Check the log file once a week.

roll-time	Time of day to roll the log file (hh:mm).	user	Not Specified	
source-ip	Source IP address to use for uploading disk log files.	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable local disk logging.	option	-	enable

Option	Description
enable	Log to local disk.
disable	Do not log to local disk.

Parameter	Description	Type	Size	Default
upload	Enable/disable uploading log files when they are rolled.	option	-	disable

Option	Description
enable	Enable uploading log files when they are rolled.
disable	Disable uploading log files when they are rolled.

Parameter	Description	Type	Size	Default
upload-delete-files	Delete log files after uploading.	option	-	enable

Option	Description
enable	Delete log files after uploading.
disable	Do not delete log files after uploading.

Parameter	Description	Type	Size	Default
upload-destination	The type of server to upload log files to. Only FTP is currently supported.	option	-	ftp-server

Option	Description
ftp-server	Upload rolled log files to an FTP server.

Parameter	Description	Type	Size	Default
upload-ssl-conn	Enable/disable encrypted FTPS communication to upload log files.	option	-	default

Option	Description
default	FTPS with high and medium encryption algorithms.
high	FTPS with high encryption algorithms.
low	FTPS with low encryption algorithms.
disable	Disable FTPS communication.

Parameter	Description	Type	Size	Default
uploaddir	The remote directory on the FTP server to upload log files to.	string	Maximum length: 63	
uploadip	IP address of the FTP server to upload log files to.	ipv4-address	Not Specified	0.0.0.0
uploadpass	Password required to log into the FTP server to upload disk log files.	password	Not Specified	
uploadport	TCP port to use for communicating with the FTP server.	integer	Minimum value: 0 Maximum value: 65535	21

Parameter	Description	Type	Size	Default
uploadsched	Set the schedule for uploading log files to the FTP server.	option	-	disable

Option	Description
disable	Upload when rolling.
enable	Scheduled upload.

Parameter	Description	Type	Size	Default
uploadtime	Time of day at which log files are uploaded if uploadsched is enabled (hh:mm or hh).	user	Not Specified	
uploadtype	Types of log files to upload. Separate multiple entries with a space.	option	-	traffic event virus webfilter IPS emailfilter dlp-archive anomaly voip dlp app-ctrl waf dns ssh ssl

Option	Description
traffic	Upload traffic log.
event	Upload event log.
virus	Upload anti-virus log.
webfilter	Upload web filter log.
IPS	Upload IPS log.
emailfilter	Upload spam filter log.
dlp-archive	Upload DLP archive.
anomaly	Upload anomaly log.
voip	Upload VoIP log.
dlp	Upload DLP log.
app-ctrl	Upload application control log.
waf	Upload web application firewall log.
dns	Upload DNS log.
ssh	Upload SSH log.
ssl	Upload SSL log.

Parameter	Description	Type	Size	Default
	Option: Description *file-filter*: Upload file-filter log. *icap*: Upload ICAP log. *ztna*: Upload ZTNA log.			
uploaduser	Username required to log into the FTP server to upload disk log files.	string	Maximum length: 35	

config log memory global-setting

Global settings for memory logging.

Syntax

```
config log memory global-setting
    set full-final-warning-threshold {integer}
    set full-first-warning-threshold {integer}
    set full-second-warning-threshold {integer}
    set max-size {integer}
end
```

config log memory global-setting

Parameter	Description	Type	Size	Default
full-final-warning-threshold	Log full final warning threshold as a percent.	integer	Minimum value: 3 Maximum value: 100	95
full-first-warning-threshold	Log full first warning threshold as a percent.	integer	Minimum value: 1 Maximum value: 98	75
full-second-warning-threshold	Log full second warning threshold as a percent.	integer	Minimum value: 2 Maximum value: 99	90
max-size	Maximum amount of memory that can be used for memory logging in bytes.	integer	Minimum value: 0 Maximum value: 268435456	67108864

config log memory setting

Settings for memory buffer.

Syntax

```
config log memory setting
    set status [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
status	Enable/disable logging to Container FortiOS memory.	option	-	disable

Option	Description
enable	Enable logging to memory.
disable	Disable logging to memory.

config log setting

Configure general log settings.

Syntax

```
config log setting
    set custom-log-fields <field-id1>, <field-id2>, ...
    set expolicy-implicit-log [enable|disable]
    set fwpolicy-implicit-log [enable|disable]
    set fwpolicy6-implicit-log [enable|disable]
    set log-policy-comment [enable|disable]
    set resolve-ip [enable|disable]
    set resolve-port [enable|disable]
    set syslog-override [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
custom-log-fields <field-id>	Custom fields to append to all log messages. Custom log field.	string	Maximum length: 35	
expolicy-implicit-log	Enable/disable explicit proxy firewall implicit policy logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable explicit proxy firewall implicit policy logging. *disable* Disable explicit proxy firewall implicit policy logging.			
fwpolicy-implicit-log	Enable/disable implicit firewall policy logging.	option	-	disable
	Option **Description** *enable* Enable implicit firewall policy logging. *disable* Disable implicit firewall policy logging.			
fwpolicy6-implicit-log	Enable/disable implicit firewall policy6 logging.	option	-	disable
	Option **Description** *enable* Enable implicit firewall policy6 logging. *disable* Disable implicit firewall policy6 logging.			
log-policy-comment	Enable/disable inserting policy comments into traffic logs.	option	-	disable
	Option **Description** *enable* Enable inserting policy comments into traffic logs. *disable* Disable inserting policy comments into traffic logs.			
resolve-ip	Enable/disable adding resolved domain names to traffic logs if possible.	option	-	disable
	Option **Description** *enable* Enable adding resolved domain names to traffic logs. *disable* Disable adding resolved domain names to traffic logs.			
resolve-port	Enable/disable adding resolved service names to traffic logs.	option	-	enable
	Option **Description** *enable* Enable adding resolved service names to traffic logs. *disable* Disable adding resolved service names to traffic logs.			
syslog-override	Enable/disable override Syslog settings.	option	-	disable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable override Syslog settings. *disable* Disable override Syslog settings.			

config log syslogd2 filter

Filters for remote system server.

Syntax

```
config log syslogd2 filter
    set forward-traffic [enable|disable]
    config free-style
        Description: Free Style Filters
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
end
```

Parameters

Parameter	Description	Type	Size	Default
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
severity	Lowest severity level to log.	option	-	information
	Option **Description** *emergency* Emergency level. *alert* Alert level. *critical* Critical level. *error* Error level. *warning* Warning level. *notification* Notification level. *information* Information level. *debug* Debug level.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option **Description** *traffic* Traffic log. *event* Event log. *virus* Antivirus log. *webfilter* Web filter log. *attack* Attack log. *app-ctrl* Application control log. *ssl* SSL log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Parameter	Description	Type	Size	Default
	Option / **Description** *include* / Include logs that match the filter. *exclude* / Exclude logs that match the filter.			
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config log syslogd2 setting

Global settings for remote syslog server.

Syntax

```
config log syslogd2 setting
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|reliable]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *high-medium* — SSL communication with high and medium encryption algorithms. *high* — SSL communication with high encryption algorithms. *low* — SSL communication with low encryption algorithms. *disable* — Disable SSL communication.			
facility	Remote syslog facility.	option	-	local7
	Option / **Description** *kernel* — Kernel messages. *user* — Random user-level messages. *mail* — Mail system. *daemon* — System daemons. *auth* — Security/authorization messages. *syslog* — Messages generated internally by syslog. *lpr* — Line printer subsystem. *news* — Network news subsystem. *uucp* — Network news subsystem. *cron* — Clock daemon. *authpriv* — Security/authorization messages (private). *ftp* — FTP daemon. *ntp* — NTP daemon. *audit* — Log audit. *alert* — Log alert. *clock* — Clock daemon. *local0* — Reserved for local use. *local1* — Reserved for local use. *local2* — Reserved for local use. *local3* — Reserved for local use. *local4* — Reserved for local use. *local5* — Reserved for local use.			

Parameter	Description	Type	Size	Default
	Option / **Description** *local6* / Reserved for local use. *local7* / Reserved for local use.			
format	Log format.	option	-	default
	Option / **Description** *default* / Syslog format. *csv* / CSV (Comma Separated Values) format. *cef* / CEF (Common Event Format) format. *rfc5424* / Syslog RFC5424 format.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* / Set outgoing interface automatically. *sdwan* / Set outgoing interface by SD-WAN or policy routing rules. *specify* / Set outgoing interface manually.			
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp
	Option / **Description** *udp* / Enable syslogging over UDP. *reliable* / Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514

Parameter	Description	Type	Size	Default
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set Syslog transmission priority to default. *low* — Set Syslog transmission priority to low.			
server	Address of remote syslog server.	string	Maximum length: 127	
source-ip	Source IP address of syslog.	string	Maximum length: 63	
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
status	Enable/disable remote syslog logging.	option	-	disable
	Option / **Description** *enable* — Log to remote syslog server. *disable* — Do not log to remote syslog server.			

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name.	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	

config log syslogd3 filter

Filters for remote system server.

Syntax

```
config log syslogd3 filter
    set forward-traffic [enable|disable]
    config free-style
        Description: Free Style Filters
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
end
```

Parameters

Parameter	Description	Type	Size	Default
forward-traffic	Enable/disable forward traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable forward traffic logging. *disable* — Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable local in or out traffic logging. *disable* — Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option / **Description** *enable* — Enable multicast traffic logging. *disable* — Disable multicast traffic logging.			
severity	Lowest severity level to log.	option	-	information

Parameter	Description	Type	Size	Default

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic

Option	Description
traffic	Traffic log.
event	Event log.
virus	Antivirus log.
webfilter	Web filter log.
attack	Attack log.
app-ctrl	Application control log.
ssl	SSL log.

filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include

Option	Description
include	Include logs that match the filter.
exclude	Exclude logs that match the filter.

id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config log syslogd3 setting

Global settings for remote syslog server.

Syntax

```
config log syslogd3 setting
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|reliable]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

Parameter	Description	Type	Size	Default
facility	Remote syslog facility.	option	-	local7

Option	Description
kernel	Kernel messages.

Parameter	Description	Type	Size	Default
	Option / **Description** *user* — Random user-level messages. *mail* — Mail system. *daemon* — System daemons. *auth* — Security/authorization messages. *syslog* — Messages generated internally by syslog. *lpr* — Line printer subsystem. *news* — Network news subsystem. *uucp* — Network news subsystem. *cron* — Clock daemon. *authpriv* — Security/authorization messages (private). *ftp* — FTP daemon. *ntp* — NTP daemon. *audit* — Log audit. *alert* — Log alert. *clock* — Clock daemon. *local0* — Reserved for local use. *local1* — Reserved for local use. *local2* — Reserved for local use. *local3* — Reserved for local use. *local4* — Reserved for local use. *local5* — Reserved for local use. *local6* — Reserved for local use. *local7* — Reserved for local use.			
format	Log format.	option	-	default
	Option / **Description** *default* — Syslog format. *csv* — CSV (Comma Separated Values) format. *cef* — CEF (Common Event Format) format. *rfc5424* — Syslog RFC5424 format.			

Parameter	Description	Type	Size	Default
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp

Option	Description
udp	Enable syslogging over UDP.
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
priority	Set log transmission priority.	option	-	default

Option	Description
default	Set Syslog transmission priority to default.
low	Set Syslog transmission priority to low.

server	Address of remote syslog server.	string	Maximum length: 127	
source-ip	Source IP address of syslog.	string	Maximum length: 63	
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default

Parameter	Description	Type	Size	Default
	Option **Description** *default* Follow system global setting. *SSLv3* SSLv3. *TLSv1* TLSv1. *TLSv1-1* TLSv1.1. *TLSv1-2* TLSv1.2.			
status	Enable/disable remote syslog logging.	option	-	disable
	Option **Description** *enable* Log to remote syslog server. *disable* Do not log to remote syslog server.			

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name.	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	

config log syslogd4 filter

Filters for remote system server.

Syntax

```
config log syslogd4 filter
    set forward-traffic [enable|disable]
    config free-style
        Description: Free Style Filters
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set local-traffic [enable|disable]
```

```
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
end
```

Parameters

Parameter	Description	Type	Size	Default
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Option	Description
enable	Enable forward traffic logging.
disable	Disable forward traffic logging.

Parameter	Description	Type	Size	Default
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable

Option	Description
enable	Enable local in or out traffic logging.
disable	Disable local in or out traffic logging.

Parameter	Description	Type	Size	Default
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable

Option	Description
enable	Enable multicast traffic logging.
disable	Disable multicast traffic logging.

Parameter	Description	Type	Size	Default
severity	Lowest severity level to log.	option	-	information

Option	Description
emergency	Emergency level.
alert	Alert level.
critical	Critical level.
error	Error level.
warning	Warning level.
notification	Notification level.
information	Information level.
debug	Debug level.

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option / **Description** *traffic* — Traffic log. *event* — Event log. *virus* — Antivirus log. *webfilter* — Web filter log. *attack* — Attack log. *app-ctrl* — Application control log. *ssl* — SSL log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option / **Description** *include* — Include logs that match the filter. *exclude* — Exclude logs that match the filter.			
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config log syslogd4 setting

Global settings for remote syslog server.

Syntax

```
config log syslogd4 setting
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
```

```
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|reliable]
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

facility	Remote syslog facility.	option	-	local7

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).

Parameter	Description	Type	Size	Default
	Option / **Description** *ftp* — FTP daemon. *ntp* — NTP daemon. *audit* — Log audit. *alert* — Log alert. *clock* — Clock daemon. *local0* — Reserved for local use. *local1* — Reserved for local use. *local2* — Reserved for local use. *local3* — Reserved for local use. *local4* — Reserved for local use. *local5* — Reserved for local use. *local6* — Reserved for local use. *local7* — Reserved for local use.			
format	Log format.	option	-	default
	Option / **Description** *default* — Syslog format. *csv* — CSV (Comma Separated Values) format. *cef* — CEF (Common Event Format) format. *rfc5424* — Syslog RFC5424 format.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			

Parameter	Description	Type	Size	Default
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp

Option	Description
udp	Enable syslogging over UDP.
reliable	Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).

Parameter	Description	Type	Size	Default
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
priority	Set log transmission priority.	option	-	default

Option	Description
default	Set Syslog transmission priority to default.
low	Set Syslog transmission priority to low.

Parameter	Description	Type	Size	Default
server	Address of remote syslog server.	string	Maximum length: 127	
source-ip	Source IP address of syslog.	string	Maximum length: 63	
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default

Option	Description
default	Follow system global setting.
SSLv3	SSLv3.
TLSv1	TLSv1.
TLSv1-1	TLSv1.1.
TLSv1-2	TLSv1.2.

Parameter	Description	Type	Size	Default
status	Enable/disable remote syslog logging.	option	-	disable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Log to remote syslog server. *disable* / Do not log to remote syslog server.			

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name.	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	

config log syslogd filter

Filters for remote system server.

Syntax

```
config log syslogd filter
    set forward-traffic [enable|disable]
    config free-style
        Description: Free Style Filters
        edit <id>
            set category [traffic|event|...]
            set filter {string}
            set filter-type [include|exclude]
        next
    end
    set local-traffic [enable|disable]
    set multicast-traffic [enable|disable]
    set severity [emergency|alert|...]
end
```

Parameters

Parameter	Description	Type	Size	Default
forward-traffic	Enable/disable forward traffic logging.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable forward traffic logging. *disable* Disable forward traffic logging.			
local-traffic	Enable/disable local in or out traffic logging.	option	-	enable
	Option **Description** *enable* Enable local in or out traffic logging. *disable* Disable local in or out traffic logging.			
multicast-traffic	Enable/disable multicast traffic logging.	option	-	enable
	Option **Description** *enable* Enable multicast traffic logging. *disable* Disable multicast traffic logging.			
severity	Lowest severity level to log.	option	-	information
	Option **Description** *emergency* Emergency level. *alert* Alert level. *critical* Critical level. *error* Error level. *warning* Warning level. *notification* Notification level. *information* Information level. *debug* Debug level.			

config free-style

Parameter	Description	Type	Size	Default
category	Log category.	option	-	traffic
	Option **Description** *traffic* Traffic log.			

Parameter	Description	Type	Size	Default
	Option **Description** *event* Event log. *virus* Antivirus log. *webfilter* Web filter log. *attack* Attack log. *app-ctrl* Application control log. *ssl* SSL log.			
filter	Free style filter string.	string	Maximum length: 1023	
filter-type	Include/exclude logs that match the filter.	option	-	include
	Option **Description** *include* Include logs that match the filter. *exclude* Exclude logs that match the filter.			
id	Entry ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config log syslogd setting

Global settings for remote syslog server.

Syntax

```
config log syslogd setting
    set certificate {string}
    config custom-field-name
        Description: Custom field name for CEF format logging.
        edit <id>
            set custom {string}
            set name {string}
        next
    end
    set enc-algorithm [high-medium|high|...]
    set facility [kernel|user|...]
    set format [default|csv|...]
    set interface {string}
    set interface-select-method [auto|sdwan|...]
    set max-log-rate {integer}
    set mode [udp|reliable]
```

```
    set port {integer}
    set priority [default|low]
    set server {string}
    set source-ip {string}
    set ssl-min-proto-version [default|SSLv3|...]
    set status [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
certificate	Certificate used to communicate with Syslog server.	string	Maximum length: 35	
enc-algorithm	Enable/disable reliable syslogging with TLS encryption.	option	-	disable

Option	Description
high-medium	SSL communication with high and medium encryption algorithms.
high	SSL communication with high encryption algorithms.
low	SSL communication with low encryption algorithms.
disable	Disable SSL communication.

facility	Remote syslog facility.	option	-	local7

Option	Description
kernel	Kernel messages.
user	Random user-level messages.
mail	Mail system.
daemon	System daemons.
auth	Security/authorization messages.
syslog	Messages generated internally by syslog.
lpr	Line printer subsystem.
news	Network news subsystem.
uucp	Network news subsystem.
cron	Clock daemon.
authpriv	Security/authorization messages (private).
ftp	FTP daemon.
ntp	NTP daemon.
audit	Log audit.

Parameter	Description	Type	Size	Default
	Option / **Description** *alert* — Log alert. *clock* — Clock daemon. *local0* — Reserved for local use. *local1* — Reserved for local use. *local2* — Reserved for local use. *local3* — Reserved for local use. *local4* — Reserved for local use. *local5* — Reserved for local use. *local6* — Reserved for local use. *local7* — Reserved for local use.			
format	Log format.	option	-	default
	Option / **Description** *default* — Syslog format. *csv* — CSV (Comma Separated Values) format. *cef* — CEF (Common Event Format) format. *rfc5424* — Syslog RFC5424 format.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto
	Option / **Description** *auto* — Set outgoing interface automatically. *sdwan* — Set outgoing interface by SD-WAN or policy routing rules. *specify* — Set outgoing interface manually.			
max-log-rate	Syslog maximum log rate in MBps (0 = unlimited).	integer	Minimum value: 0 Maximum value: 100000	0
mode	Remote syslog logging over UDP/Reliable TCP.	option	-	udp

Parameter	Description	Type	Size	Default
	Option / **Description** *udp* — Enable syslogging over UDP. *reliable* — Enable reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP).			
port	Server listen port.	integer	Minimum value: 0 Maximum value: 65535	514
priority	Set log transmission priority.	option	-	default
	Option / **Description** *default* — Set Syslog transmission priority to default. *low* — Set Syslog transmission priority to low.			
server	Address of remote syslog server.	string	Maximum length: 127	
source-ip	Source IP address of syslog.	string	Maximum length: 63	
ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option / **Description** *default* — Follow system global setting. *SSLv3* — SSLv3. *TLSv1* — TLSv1. *TLSv1-1* — TLSv1.1. *TLSv1-2* — TLSv1.2.			
status	Enable/disable remote syslog logging.	option	-	disable
	Option / **Description** *enable* — Log to remote syslog server. *disable* — Do not log to remote syslog server.			

config custom-field-name

Parameter	Description	Type	Size	Default
custom	Field custom name.	string	Maximum length: 35	
id	Entry ID.	integer	Minimum value: 0 Maximum value: 255	0
name	Field name.	string	Maximum length: 35	

report

This section includes syntax for the following commands:

- config report setting on page 154

config report setting

Report setting configuration.

Syntax

```
config report setting
    set report-source {option1}, {option2}, ...
end
```

Parameters

Parameter	Description	Type	Size	Default
report-source	Report log source.	option	-	forward-traffic

Option	Description
forward-traffic	Report includes forward traffic logs.
sniffer-traffic	Report includes sniffer traffic logs.
local-deny-traffic	Report includes local deny traffic logs.

router

This section includes syntax for the following commands:

- config router static on page 155

config router static

Configure IPv4 static routing tables.

Syntax

```
config router static
    edit <seq-num>
        set comment {var-string}
        set device {string}
        set distance {integer}
        set dst {ipv4-classnet}
        set dstaddr {string}
        set gateway {ipv4-address}
        set priority {integer}
        set src {ipv4-address}
        set status [enable|disable]
        set weight {integer}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
device	Gateway out interface or tunnel.	string	Maximum length: 35	
distance	Administrative distance.	integer	Minimum value: 1 Maximum value: 255	10
dst	Destination IP and mask for this route.	ipv4-classnet	Not Specified	0.0.0.0 0.0.0.0
dstaddr	Name of firewall address or address group.	string	Maximum length: 79	
gateway	Gateway IP for this route.	ipv4-address	Not Specified	0.0.0.0

Parameter	Description	Type	Size	Default
priority	Administrative priority.	integer	Minimum value: 1 Maximum value: 65535	1
seq-num	Sequence number.	integer	Minimum value: 0 Maximum value: 4294967295	0
src	Source address for this route.	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable this static route.	option	-	enable

Option	Description
enable	Enable static route.
disable	Disable static route.

weight	Administrative weight.	integer	Minimum value: 0 Maximum value: 255	0

system

This section includes syntax for the following commands:

- config system admin on page 157
- config system api-user on page 157
- config system autoupdate schedule on page 158
- config system dns on page 159
- config system external-resource on page 159
- config system fortiguard on page 161
- config system global on page 163
- config system interface on page 164
- config system ips on page 165
- config system replacemsg-group on page 165
- config system replacemsg-image on page 169
- config system replacemsg fortiguard-wf on page 169
- config system replacemsg http on page 170
- config system replacemsg utm on page 171
- config system settings on page 172

config system admin

Configure admin users.

Syntax

```
config system admin
    edit <name>
        set passwd {password}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
name	Admin user name.	string	Maximum length: 15	
passwd	Admin user password.	password	Not Specified	

config system api-user

Configure API users.

Syntax

```
config system api-user
    edit <name>
    next
end
```

config system api-user

Parameter	Description	Type	Size	Default
name	API user name.	string	Maximum length: 15	

config system autoupdate schedule

Configure update schedule.

Syntax

```
config system autoupdate schedule
    set day [Sunday|Monday|...]
    set frequency [every|daily|...]
    set status [enable|disable]
    set time {user}
end
```

Parameters

Parameter	Description	Type	Size	Default
day	Update day.	option	-	Monday

Option	Description
Sunday	Update every Sunday.
Monday	Update every Monday.
Tuesday	Update every Tuesday.
Wednesday	Update every Wednesday.
Thursday	Update every Thursday.
Friday	Update every Friday.
Saturday	Update every Saturday.

frequency	Update frequency.	option	-	automatic

Parameter	Description	Type	Size	Default
	Option **Description** *every* Time interval. *daily* Every day. *weekly* Every week. *automatic* Update automatically within every one hour period.			
status	Enable/disable scheduled updates.	option	-	enable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
time	Update time.	user	Not Specified	

config system dns

Configure DNS.

Syntax

```
config system dns
    set primary {ipv4-address}
    set secondary {ipv4-address}
end
```

Parameters

Parameter	Description	Type	Size	Default
primary	Primary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0
secondary	Secondary DNS server IP address.	ipv4-address	Not Specified	0.0.0.0

config system external-resource

Configure external resource.

Syntax

```
config system external-resource
    edit <name>
```

```
        set category {integer}
        set comments {var-string}
        set interface {string}
        set interface-select-method [auto|sdwan|...]
        set password {password}
        set refresh-rate {integer}
        set resource {string}
        set source-ip {ipv4-address}
        set status [enable|disable]
        set type [category|address|...]
        set user-agent {string}
        set username {string}
        set uuid {uuid}
    next
end
```

config system external-resource

Parameter	Description	Type	Size	Default
category	User resource category 192 - 221.	integer	Minimum value: 192 Maximum value: 221	0
comments	Comment.	var-string	Maximum length: 255	
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	
interface-select-method	Specify how to select outgoing interface to reach server.	option	-	auto

Option	Description
auto	Set outgoing interface automatically.
sdwan	Set outgoing interface by SD-WAN or policy routing rules.
specify	Set outgoing interface manually.

name	External resource name.	string	Maximum length: 35	
password	HTTP basic authentication password.	password	Not Specified	
refresh-rate	Time interval to refresh external resource.	integer	Minimum value: 1 Maximum value: 43200	5

Parameter	Description	Type	Size	Default
resource	URI of external resource.	string	Maximum length: 511	
source-ip	Source IPv4 address used to communicate with server.	ipv4-address	Not Specified	0.0.0.0
status	Enable/disable user resource.	option	-	enable
	Option / **Description** *enable* — Enable user resource. *disable* — Disable user resource.			
type	User resource type.	option	-	category
	Option / **Description** *category* — FortiGuard category. *address* — Firewall IP address. *domain* — Domain Name. *malware* — Malware hash.			
user-agent	HTTP User-Agent header.	string	Maximum length: 127	curl/7.58.0
username	HTTP basic authentication user name.	string	Maximum length: 64	
uuid	Universally Unique Identifier (UUID; automatically assigned but can be manually reset).	uuid	Not Specified	00000000-0000-0000-0000-000000000000

config system fortiguard

Configure FortiGuard services.

Syntax

```
config system fortiguard
    set fortiguard-anycast [enable|disable]
    set fortiguard-anycast-source [fortinet|aws|...]
    set interface {string}
    set update-extdb [enable|disable]
    set update-ffdb [enable|disable]
    set webfilter-cache [enable|disable]
    set webfilter-cache-ttl {integer}
    set webfilter-expiration {string}
    set webfilter-force-off [enable|disable]
    set webfilter-license {string}
```

```
    set webfilter-timeout {integer}
end
```

Parameters

Parameter	Description	Type	Size	Default
fortiguard-anycast	Enable/disable use of FortiGuard's Anycast network.	option	-	enable
	Option / **Description** *enable* — Enable use of FortiGuard's Anycast network. *disable* — Disable use of FortiGuard's Anycast network.			
fortiguard-anycast-source	Configure which of Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. Default is Fortinet.	option	-	fortinet
	Option / **Description** *fortinet* — Use Fortinet's servers to provide FortiGuard services in FortiGuard's anycast network. *aws* — Use Fortinet's AWS servers to provide FortiGuard services in FortiGuard's anycast network. *debug* — Use Fortinet's internal test servers to provide FortiGuard services in FortiGuard's anycast network.			
interface	Specify outgoing interface to reach server.	string	Maximum length: 15	any
update-extdb	Enable/disable external resource update.	option	-	enable
	Option / **Description** *enable* — Enable external resource update. *disable* — Disable external resource update.			
update-ffdb	Enable/disable Internet Service Database update.	option	-	enable
	Option / **Description** *enable* — Enable Internet Service Database update. *disable* — Disable Internet Service Database update.			
webfilter-cache	Enable/disable FortiGuard web filter caching.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable FortiGuard web filter caching. *disable* / Disable FortiGuard web filter caching.			
webfilter-cache-ttl	Time-to-live for web filter cache entries in seconds.	integer	Minimum value: 300 Maximum value: 86400	3600
webfilter-expiration	Expiration date of the FortiGuard web filter contract. Read-only.	string	Maximum length: -	
webfilter-force-off	Enable/disable turning off the FortiGuard web filtering service.	option	-	disable
	Option / **Description** *enable* / Turn off the FortiGuard web filtering service. *disable* / Allow the FortiGuard web filtering service to operate.			
webfilter-license	Web filter license status. Read-only.	string	Maximum length: -	
webfilter-timeout	Web filter query time out.	integer	Minimum value: 1 Maximum value: 30	15

config system global

Configure global attributes.

Syntax

```
config system global
    set admin-port {integer}
    set admin-server-cert {string}
    set admin-sport {integer}
    set cert-chain-max {integer}
    set remoteauthtimeout {integer}
end
```

Parameters

Parameter	Description	Type	Size	Default
admin-port	REST API access port for HTTP. 0 disables HTTP.	integer	Minimum value: 0 Maximum value: 65535	0
admin-server-cert	Server certificate that Container FortiOS uses for HTTPS administrative connections.	string	Maximum length: -	Fortinet_ GUI_Server
admin-sport	REST API access port for HTTPS. 0 disables HTTPS.	integer	Minimum value: 0 Maximum value: 65535	443
cert-chain-max	Maximum number of certificates that can be traversed in a certificate chain.	integer	Minimum value: 1 Maximum value: 2147483647	8
remoteauthtimeout	Number of seconds that Container FortiOS waits for responses from remote authentication servers.	integer	Minimum value: 1 Maximum value: 300	5

config system interface

Configure interfaces.

Syntax

```
config system interface
    edit <name>
        set ip {ipv4-classnet-host}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
ip	Interface IPv4 address and subnet mask, syntax: X.X.X.X/24.	ipv4-classnet-host	Not Specified	0.0.0.0 0.0.0.0
name	Name.	string	Maximum length: 15	

config system ips

Configure IPS system settings.

Syntax

```
config system ips
    set override-signature-hold-by-id [enable|disable]
    set signature-hold-time {user}
end
```

Parameters

Parameter	Description	Type	Size	Default
override-signature-hold-by-id	Enable/disable override of hold of triggering signatures that are specified by IDs regardless of hold.	option	-	enable

Option	Description
enable	Allow the signatures specified by IDs to be triggered even if they are on hold.
disable	Do not trigger the signatures that are on hold.

Parameter	Description	Type	Size	Default
signature-hold-time	Time to hold and monitor IPS signatures. Format <#d##h>.	user	Not Specified	0h

config system replacemsg-group

Configure replacement message groups.

Syntax

```
config system replacemsg-group
    edit <name>
        set comment {var-string}
        config custom-message
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set format [none|text|...]
                set header [none|http|...]
            next
        end
        config fortiguard-wf
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set format [none|text|...]
                set header [none|http|...]
            next
```

```
        end
        set group-type {option}
        config http
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set format [none|text|...]
                set header [none|http|...]
            next
        end
        config utm
            Description: Replacement message table entries.
            edit <msg-type>
                set buffer {var-string}
                set format [none|text|...]
                set header [none|http|...]
            next
        end
    next
end
```

config system replacemsg-group

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
group-type	Group type.	option	-	utm

Option	Description
utm	For use with UTM settings in firewall policies.

Parameter	Description	Type	Size	Default
name	Group name.	string	Maximum length: 35	

config custom-message

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

Parameter	Description	Type	Size	Default
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	

config fortiguard-wf

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none

Option	Description
none	No format type.
text	Text format.
html	HTML format.

Parameter	Description	Type	Size	Default
header	Header flag.	option	-	none

Option	Description
none	No header type.
http	HTTP
8bit	8 bit.

Parameter	Description	Type	Size	Default
msg-type	Message type.	string	Maximum length: 28	

config http

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	none
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			
header	Header flag.	option	-	none
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
msg-type	Message type.	string	Maximum length: 28	

config utm

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	none
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			
header	Header flag.	option	-	none
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg-image

Configure replacement message images.

Syntax

```
config system replacemsg-image
    edit <name>
        set image-base64 {var-string}
        set image-type [gif|jpg|...]
    next
end
```

config system replacemsg-image

Parameter	Description	Type	Size	Default
image-base64	Image data.	var-string	Maximum length: 32768	
image-type	Image type.	option	-	png

Option	Description
gif	GIF image.
jpg	JPEG image.
tiff	TIFF image.
png	PNG image.

name	Image name.	string	Maximum length: 23	

config system replacemsg fortiguard-wf

Replacement messages.

Syntax

```
config system replacemsg fortiguard-wf
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

config system replacemsg fortiguard-wf

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			
header	Header flag.	option	-	
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg http

Replacement messages.

Syntax

```
config system replacemsg http
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	

Parameter	Description	Type	Size	Default
format	Format flag.	option	-	
	Option / **Description** *none* — No format type. *text* — Text format. *html* — HTML format.			
header	Header flag.	option	-	
	Option / **Description** *none* — No header type. *http* — HTTP *8bit* — 8 bit.			
msg-type	Message type.	string	Maximum length: 28	

config system replacemsg utm

Replacement messages.

Syntax

```
config system replacemsg utm
    edit <msg-type>
        set buffer {var-string}
        set format [none|text|...]
        set header [none|http|...]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
buffer	Message string.	var-string	Maximum length: 32768	
format	Format flag.	option	-	
	Option / **Description** *none* — No format type.			

Parameter	Description	Type	Size	Default
	Option **Description** *text* Text format. *html* HTML format.			
header	Header flag.	option	-	
	Option **Description** *none* No header type. *http* HTTP *8bit* 8 bit.			
msg-type	Message type.	string	Maximum length: 28	

config system settings

Configure settings.

Syntax

```
config system settings
    set central-nat [enable|disable]
    set ngfw-mode [profile-based|policy-based]
    set tcp-session-without-syn [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
central-nat	Enable/disable central NAT.	option	-	disable
	Option **Description** *enable* Enable central NAT. *disable* Disable central NAT.			
ngfw-mode	Next Generation Firewall (NGFW) mode.	option	-	profile-based
	Option **Description** *profile-based* Application and web-filtering are configured using profiles applied to policy entries.			

Parameter	Description	Type	Size	Default
	Option **Description** *policy-based* Application and web-filtering are configured as policy match conditions.			
tcp-session-without-syn	Enable/disable allowing TCP session without SYN flags.	option	-	disable
	Option **Description** *enable* Allow TCP session without SYN flags. *disable* Do not allow TCP session without SYN flags.			

vpn

This section includes syntax for the following commands:

- config vpn certificate ca on page 174
- config vpn certificate local on page 175
- config vpn certificate setting on page 175
- config vpn ipsec phase1-interface on page 176
- config vpn ipsec phase2-interface on page 181

config vpn certificate ca

CA certificate.

Syntax

```
config vpn certificate ca
    edit <name>
        set ca {user}
        set source [factory|user|...]
        set ssl-inspection-trusted [enable|disable]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
ca	CA certificate as a PEM file.	user	Not Specified	
name	Name.	string	Maximum length: 35	
source	CA certificate source type.	option	-	user
	Option / **Description** *factory* — Factory installed certificate. *user* — User generated certificate. *bundle* — Bundle file certificate.			
ssl-inspection-trusted	Enable/disable this CA as a trusted CA for SSL inspection.	option	-	enable

Parameter	Description	Type	Size	Default
	Option — **Description** *enable* — Trusted CA for SSL inspection. *disable* — Untrusted CA for SSL inspection.			

config vpn certificate local

Local keys and certificates.

Syntax

```
config vpn certificate local
    edit <name>
        set certificate {user}
        set comments {string}
        set password {password}
        set private-key {user}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
certificate	PEM format certificate.	user	Not Specified	
comments	Comment.	string	Maximum length: 511	
name	Name.	string	Maximum length: 35	
password	Password as a PEM file.	password	Not Specified	
private-key	PEM format key, encrypted with a password.	user	Not Specified	

config vpn certificate setting

VPN certificate setting.

Syntax

```
config vpn certificate setting
    set ocsp-status [enable|disable]
```

```
    set strict-ocsp-check [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
ocsp-status	Enable/disable receiving certificates using the OCSP.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
strict-ocsp-check	Enable/disable strict mode OCSP checking.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

config vpn ipsec phase1-interface

Configure VPN remote gateway.

Syntax

```
config vpn ipsec phase1-interface
    edit <name>
        set add-route [disable|enable]
        set authmethod [psk|signature]
        set auto-negotiate [enable|disable]
        set dhgrp {option1}, {option2}, ...
        set dpd [disable|on-idle|...]
        set dpd-retrycount {integer}
        set dpd-retryinterval {integer}
        set fragmentation [enable|disable]
        set fragmentation-mtu {integer}
        set interface {string}
        set keepalive {integer}
        set keylife {integer}
        set localid {string}
        set localid-type [auto|fqdn|...]
        set mode-cfg [disable|enable]
        set peertype [any|one|...]
        set proposal {option1}, {option2}, ...
        set psksecret {password-3}
        set reauth [disable|enable]
        set rekey [enable|disable]
        set remote-gw {ipv4-address}
```

```
    next
end
```

config vpn ipsec phase1-interface

Parameter	Description	Type	Size	Default
add-route	Enable/disable control addition of a route to peer destination selector.	option	-	enable

Option	Description
disable	Do not add a route to destination of peer selector.
enable	Add route to destination of peer selector.

Parameter	Description	Type	Size	Default
authmethod	Authentication method.	option	-	psk

Option	Description
psk	PSK authentication method.
signature	Signature authentication method.

Parameter	Description	Type	Size	Default
auto-negotiate	Enable/disable automatic initiation of IKE SA negotiation.	option	-	enable

Option	Description
enable	Enable automatic initiation of IKE SA negotiation.
disable	Disable automatic initiation of IKE SA negotiation.

Parameter	Description	Type	Size	Default
dhgrp	DH group.	option	-	14

Option	Description
2	DH Group 2.
5	DH Group 5.
14	DH Group 14.
15	DH Group 15.
16	DH Group 16.
17	DH Group 17.
18	DH Group 18.
19	DH Group 19.
20	DH Group 20.
21	DH Group 21.

Parameter	Description	Type	Size	Default
dpd	Dead Peer Detection mode.	option	-	on-demand

Parameter	Description	Type	Size	Default
	Option / **Description** *disable* / Disable Dead Peer Detection. *on-idle* / Trigger Dead Peer Detection when IPsec is idle. *on-demand* / Trigger Dead Peer Detection when IPsec traffic is sent but no reply is received from the peer.			
dpd-retrycount	Number of DPD retry attempts.	integer	Minimum value: 0 Maximum value: 10	3
dpd-retryinterval	DPD retry interval.	integer	Minimum value: 0 Maximum value: 3600	20
fragmentation	Enable/disable fragment IKE message on re-transmission.	option	-	enable
	Option / **Description** *enable* / Enable intra-IKE fragmentation support on re-transmission. *disable* / Disable intra-IKE fragmentation support.			
fragmentation-mtu	IKE fragmentation MTU.	integer	Minimum value: 500 Maximum value: 16000	1200
interface	Local physical, aggregate, or VLAN outgoing interface.	string	Maximum length: 35	
keepalive	NAT-T keep alive interval.	integer	Minimum value: 10 Maximum value: 900	10
keylife	Time to wait in seconds before phase 1 encryption key expires.	integer	Minimum value: 120 Maximum value: 172800	86400
localid	Local ID.	string	Maximum length: 63	
localid-type	Local ID type.	option	-	auto

Parameter	Description	Type	Size	Default
	Option / **Description** *auto* — Select ID type automatically. *fqdn* — Use fully qualified domain name. *user-fqdn* — Use user fully qualified domain name. *keyid* — Use key-id string. *address* — Use local IP address. *asn1dn* — Use ASN.1 distinguished name.			
mode-cfg	Enable/disable configuration method.	option	-	disable
	Option / **Description** *disable* — Disable Configuration Method. *enable* — Enable Configuration Method.			
peertype	Accept this peer type.	option	-	peer
	Option / **Description** *any* — Accept any peer ID. *one* — Accept this peer ID. *dialup* — Accept peer ID in dialup group. *peer* — Accept this peer certificate. *peergrp* — Accept this peer certificate group.			
proposal	Phase1 proposal.	option	-	aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-prfsha256
	Option / **Description** *aes128-sha1* — aes128-sha1 *aes128-sha256* — aes128-sha256 *aes128-sha384* — aes128-sha384 *aes128-sha512* — aes128-sha512			

Parameter	Description	Type	Size	Default
	Option / **Description** *aes128gcm-prfsha1* / aes128gcm-prfsha1 *aes128gcm-prfsha256* / aes128gcm-prfsha256 *aes128gcm-prfsha384* / aes128gcm-prfsha384 *aes128gcm-prfsha512* / aes128gcm-prfsha512 *aes192-sha1* / aes192-sha1 *aes192-sha256* / aes192-sha256 *aes192-sha384* / aes192-sha384 *aes192-sha512* / aes192-sha512 *aes256-sha1* / aes256-sha1 *aes256-sha256* / aes256-sha256 *aes256-sha384* / aes256-sha384 *aes256-sha512* / aes256-sha512 *aes256gcm-prfsha1* / aes256gcm-prfsha1 *aes256gcm-prfsha256* / aes256gcm-prfsha256 *aes256gcm-prfsha384* / aes256gcm-prfsha384 *aes256gcm-prfsha512* / aes256gcm-prfsha512 *chacha20poly1305-prfsha1* / chacha20poly1305-prfsha1 *chacha20poly1305-prfsha256* / chacha20poly1305-prfsha256 *chacha20poly1305-prfsha384* / chacha20poly1305-prfsha384 *chacha20poly1305-prfsha512* / chacha20poly1305-prfsha512			
psksecret	Pre-shared secret for PSK authentication (ASCII string or hexadecimal encoded with a leading 0x).	password-3	Not Specified	
reauth	Enable/disable re-authentication upon IKE SA lifetime expiration. **Option** / **Description** *disable* / Disable IKE SA re-authentication. *enable* / Enable IKE SA re-authentication.	option	-	disable
rekey	Enable/disable phase1 rekey.	option	-	enable

Parameter	Description	Type	Size	Default
	Option / **Description** *enable* / Enable phase1 rekey. *disable* / Disable phase1 rekey.			
remote-gw	IPv4 address of the remote gateway's external interface.	ipv4-address	Not Specified	0.0.0.0

config vpn ipsec phase2-interface

Configure VPN autokey tunnel.

Syntax

```
config vpn ipsec phase2-interface
    edit <name>
        set dst-end-ip {ipv4-address-any}
        set dst-name {string}
        set dst-start-ip {ipv4-address-any}
        set dst-subnet {ipv4-classnet-any}
        set keylifeseconds {integer}
        set phase1name {string}
        set proposal {option1}, {option2}, ...
        set src-addr-type [subnet|range|...]
        set src-end-ip {ipv4-address-any}
        set src-name {string}
        set src-start-ip {ipv4-address-any}
        set src-subnet {ipv4-classnet-any}
    next
end
```

config vpn ipsec phase2-interface

Parameter	Description	Type	Size	Default
dst-end-ip	Remote proxy ID IPv4 end.	ipv4-address-any	Not Specified	0.0.0.0
dst-name	Remote proxy ID name.	string	Maximum length: 79	
dst-start-ip	Remote proxy ID IPv4 start.	ipv4-address-any	Not Specified	0.0.0.0
dst-subnet	Remote proxy ID IPv4 subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0

Parameter	Description	Type	Size	Default
keylifeseconds	Phase2 key life in time in seconds.	integer	Minimum value: 120 Maximum value: 172800	43200
phase1name	Phase 1 determines the options required for phase 2.	string	Maximum length: 15	
proposal	Phase2 proposal.	option	-	aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305

Option	Description
aes128-sha1	aes128-sha1
aes128-sha256	aes128-sha256
aes128-sha384	aes128-sha384
aes128-sha512	aes128-sha512
aes192-sha1	aes192-sha1
aes192-sha256	aes192-sha256
aes192-sha384	aes192-sha384
aes192-sha512	aes192-sha512
aes256-sha1	aes256-sha1
aes256-sha256	aes256-sha256
aes256-sha384	aes256-sha384
aes256-sha512	aes256-sha512
aes128gcm	aes128gcm
aes256gcm	aes256gcm
chacha20poly1305	chacha20poly1305

src-addr-type	Local proxy ID type.	option	-	subnet

Option	Description
subnet	IPv4 subnet.

Parameter	Description	Type	Size	Default
	Option **Description** *range* IPv4 range. *ip* IPv4 IP. *name* IPv4 firewall address or group name. *subnet6* IPv6 subnet. *range6* IPv6 range. *ip6* IPv6 IP. *name6* IPv6 firewall address or group name.			
src-end-ip	Local proxy ID end.	ipv4-address-any	Not Specified	0.0.0.0
src-name	Local proxy ID name.	string	Maximum length: 79	
src-start-ip	Local proxy ID start.	ipv4-address-any	Not Specified	0.0.0.0
src-subnet	Local proxy ID subnet.	ipv4-classnet-any	Not Specified	0.0.0.0 0.0.0.0

webfilter

This section includes syntax for the following commands:

- config webfilter content-header on page 184
- config webfilter content on page 185
- config webfilter fortiguard on page 187
- config webfilter ftgd-local-cat on page 189
- config webfilter ftgd-local-rating on page 190
- config webfilter ips-urlfilter-cache-setting on page 190
- config webfilter ips-urlfilter-setting on page 191
- config webfilter ips-urlfilter-setting6 on page 192
- config webfilter profile on page 192
- config webfilter search-engine on page 202
- config webfilter urlfilter on page 203

config webfilter content-header

Configure content types used by Web filter.

Syntax

```
config webfilter content-header
    edit <id>
        set comment {var-string}
        config entries
            Description: Configure content types used by web filter.
            edit <pattern>
                set action [block|allow|...]
                set category {user}
            next
        end
        set name {string}
    next
end
```

config webfilter content-header

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default
action	Action to take for this content type.	option	-	allow

Option	Description
block	Block content type.
allow	Allow content type.
exempt	Exempt content type.

Parameter	Description	Type	Size	Default
category	Categories that this content type applies to.	user	Not Specified	all
pattern	Content type (regular expression).	string	Maximum length: 31	

config webfilter content

Configure Web filter banned word table.

Syntax

```
config webfilter content
    edit <id>
        set comment {var-string}
        config entries
            Description: Configure banned word entries.
            edit <name>
                set action [block|exempt]
                set lang [western|simch|...]
                set pattern-type [wildcard|regexp]
                set score {integer}
                set status [enable|disable]
            next
        end
        set name {string}
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
name	Name of table.	string	Maximum length: 63	

config entries

Parameter	Description	Type	Size	Default
action	Block or exempt word when a match is found.	option	-	block
	Option / **Description** *block* — Block matches. *exempt* — Exempt matches.			
lang	Language of banned word.	option	-	western
	Option / **Description** *western* — Western. *simch* — Simplified Chinese. *trach* — Traditional Chinese. *japanese* — Japanese. *korean* — Korean. *french* — French. *thai* — Thai. *spanish* — Spanish. *cyrillic* — Cyrillic.			
name	Banned word.	string	Maximum length: 127	
pattern-type	Banned word pattern type: wildcard pattern or Perl regular expression.	option	-	wildcard

Parameter	Description	Type	Size	Default
	Option / **Description** *wildcard* / Wildcard pattern. *regexp* / Perl regular expression.			
score	Score, to be applied every time the word appears on a web page.	integer	Minimum value: 0 Maximum value: 4294967295	10
status	Enable/disable banned word.	option	-	disable
	Option / **Description** *enable* / Enable setting. *disable* / Disable setting.			

config webfilter fortiguard

Configure FortiGuard Web Filter service.

Syntax

```
config webfilter fortiguard
    set cache-mem-percent {integer}
    set cache-mode [ttl|db-ver]
    set cache-prefix-match [enable|disable]
    set close-ports [enable|disable]
    set ovrd-auth-https [enable|disable]
    set ovrd-auth-port-http {integer}
    set ovrd-auth-port-https {integer}
    set ovrd-auth-port-https-flow {integer}
    set ovrd-auth-port-warning {integer}
    set request-packet-size-limit {integer}
    set warn-auth-https [enable|disable]
end
```

Parameters

Parameter	Description	Type	Size	Default
cache-mem-percent	Maximum percentage of available memory allocated to caching.	integer	Minimum value: 1 Maximum value: 15	2
cache-mode	Cache entry expiration mode.	option	-	ttl

Parameter	Description	Type	Size	Default
	Option **Description** *ttl* Expire cache items by time-to-live. *db-ver* Expire cache items when the server DB version changes.			
cache-prefix-match	Enable/disable prefix matching in the cache.	option	-	enable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
close-ports	Close ports used for HTTP/HTTPS override authentication and disable user overrides.	option	-	disable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
ovrd-auth-https	Enable/disable use of HTTPS for override authentication.	option	-	enable
	Option **Description** *enable* Enable setting. *disable* Disable setting.			
ovrd-auth-port-http	Port to use for FortiGuard Web Filter HTTP override authentication	integer	Minimum value: 0 Maximum value: 65535	8008
ovrd-auth-port-https	Port to use for FortiGuard Web Filter HTTPS override authentication in proxy mode.	integer	Minimum value: 0 Maximum value: 65535	8010
ovrd-auth-port-https-flow	Port to use for FortiGuard Web Filter HTTPS override authentication in flow mode.	integer	Minimum value: 0 Maximum value: 65535	8015

Parameter	Description	Type	Size	Default
ovrd-auth-port-warning	Port to use for FortiGuard Web Filter Warning override authentication.	integer	Minimum value: 0 Maximum value: 65535	8020
request-packet-size-limit	Limit size of URL request packets sent to FortiGuard server.	integer	Minimum value: 576 Maximum value: 10000	0
warn-auth-https	Enable/disable use of HTTPS for warning and authentication.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

config webfilter ftgd-local-cat

Configure FortiGuard Web Filter local categories.

Syntax

```
config webfilter ftgd-local-cat
    edit <desc>
        set id {integer}
        set status [enable|disable]
    next
end
```

config webfilter ftgd-local-cat

Parameter	Description	Type	Size	Default
desc	Local category description.	string	Maximum length: 79	
id	Local category ID.	integer	Minimum value: 140 Maximum value: 191	0
status	Enable/disable the local category.	option	-	enable

Parameter	Description	Type	Size	Default
	Option **Description** *enable* Enable the local category. *disable* Disable the local category.			

config webfilter ftgd-local-rating

Configure local FortiGuard Web Filter local ratings.

Syntax

```
config webfilter ftgd-local-rating
    edit <url>
        set comment {var-string}
        set rating {user}
        set status [enable|disable]
    next
end
```

config webfilter ftgd-local-rating

Parameter	Description	Type	Size	Default
comment	Comment.	var-string	Maximum length: 255	
rating	Local rating.	user	Not Specified	
status	Enable/disable local rating.	option	-	enable
	Option **Description** *enable* Enable local rating. *disable* Disable local rating.			
url	URL to rate locally.	string	Maximum length: 511	

config webfilter ips-urlfilter-cache-setting

Configure IPS URL filter cache settings.

Syntax

```
config webfilter ips-urlfilter-cache-setting
    set dns-retry-interval {integer}
```

```
    set extended-ttl {integer}
end
```

config webfilter ips-urlfilter-cache-setting

Parameter	Description	Type	Size	Default
dns-retry-interval	Retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. 0 means use DNS server's TTL only.	integer	Minimum value: 0 Maximum value: 2147483	0
extended-ttl	Extend time to live beyond reported by DNS. 0 means use DNS server's TTL	integer	Minimum value: 0 Maximum value: 2147483	0

config webfilter ips-urlfilter-setting

Configure IPS URL filter settings.

Syntax

```
config webfilter ips-urlfilter-setting
    set device {string}
    set distance {integer}
    set gateway {ipv4-address}
    set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway	Gateway IP address for this route.	ipv4-address	Not Specified	0.0.0.0
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IP address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter ips-urlfilter-setting6

Configure IPS URL filter settings for IPv6.

Syntax

```
config webfilter ips-urlfilter-setting6
    set device {string}
    set distance {integer}
    set gateway6 {ipv6-address}
    set geo-filter {var-string}
end
```

config webfilter ips-urlfilter-setting6

Parameter	Description	Type	Size	Default
device	Interface for this route.	string	Maximum length: 35	
distance	Administrative distance for this route.	integer	Minimum value: 1 Maximum value: 255	1
gateway6	Gateway IPv6 address for this route.	ipv6-address	Not Specified	::
geo-filter	Filter based on geographical location. Route will NOT be installed if the resolved IPv6 address belongs to the country in the filter.	var-string	Maximum length: 255	

config webfilter profile

Configure Web filter profiles.

Syntax

```
config webfilter profile
    edit <name>
        set comment {var-string}
        set extended-log [enable|disable]
        config ftgd-wf
            Description: FortiGuard Web Filter settings.
            set exempt-quota {user}
            config filters
                Description: FortiGuard filters.
                edit <id>
                    set action [block|authenticate|...]
                    set auth-usr-grp <name1>, <name2>, ...
                    set category {integer}
                    set log [enable|disable]
```

```
                    set override-replacemsg {string}
                    set warn-duration {user}
                    set warning-duration-type [session|timeout]
                    set warning-prompt [per-domain|per-category]
                next
            end
            set max-quota-timeout {integer}
            set options {option1}, {option2}, ...
            set ovrd {user}
            config quota
                Description: FortiGuard traffic quota settings.
                edit <id>
                    set category {user}
                    set duration {user}
                    set override-replacemsg {string}
                    set type [time|traffic]
                    set unit [B|KB|...]
                    set value {integer}
                next
            end
            set rate-crl-urls [disable|enable]
            set rate-css-urls [disable|enable]
            set rate-javascript-urls [disable|enable]
        end
        set https-replacemsg [enable|disable]
        set log-all-url [enable|disable]
        set options {option1}, {option2}, ...
        config override
            Description: Web Filter override settings.
            set ovrd-cookie [allow|deny]
            set ovrd-dur {user}
            set ovrd-dur-mode [constant|ask]
            set ovrd-scope [user|user-group|...]
            set ovrd-user-group <name1>, <name2>, ...
            set profile <name1>, <name2>, ...
            set profile-attribute [User-Name|NAS-IP-Address|...]
            set profile-type [list|radius]
        end
        set post-action [normal|block]
        set replacemsg-group {string}
        config web
            Description: Web content filtering settings.
            set bword-table {integer}
            set bword-threshold {integer}
            set content-header-list {integer}
            set urlfilter-table {integer}
        end
        set web-content-log [enable|disable]
        set web-filter-command-block-log [enable|disable]
        set web-filter-cookie-log [enable|disable]
        set web-ftgd-err-log [enable|disable]
        set web-ftgd-quota-usage [enable|disable]
        set web-invalid-domain-log [enable|disable]
        set web-url-log [enable|disable]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
extended-log	Enable/disable extended logging for web filtering.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
https-replacemsg	Enable replacement messages for HTTPS.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
log-all-url	Enable/disable logging all URLs visited.	option	-	disable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
name	Profile name.	string	Maximum length: 35	
options	Options.	option	-	

Option	Description
activexfilter	ActiveX filter.
cookiefilter	Cookie filter.
javafilter	Java applet filter.
block-invalid-url	Block sessions contained an invalid domain name.
jscript	Javascript block.
js	JS block.
vbs	VB script block.
unknown	Unknown script block.
intrinsic	Intrinsic script block.

Parameter	Description	Type	Size	Default
	Option **Description** *wf-referer* Referring block. *wf-cookie* Cookie block.			
post-action	Action taken for HTTP POST traffic. **Option** **Description** *normal* Normal, POST requests are allowed. *block* POST requests are blocked.	option	-	normal
replacemsg-group	Replacement message group.	string	Maximum length: 35	
web-content-log	Enable/disable logging logging blocked web content. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	enable
web-filter-command-block-log	Enable/disable logging blocked commands. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	enable
web-filter-cookie-log	Enable/disable logging cookie filtering. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	enable
web-ftgd-err-log	Enable/disable logging rating errors. **Option** **Description** *enable* Enable setting. *disable* Disable setting.	option	-	enable

Parameter	Description	Type	Size	Default
web-ftgd-quota-usage	Enable/disable logging daily quota usage.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-invalid-domain-log	Enable/disable logging invalid domain names.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

Parameter	Description	Type	Size	Default
web-url-log	Enable/disable logging URL filtering.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

config ftgd-wf

Parameter	Description	Type	Size	Default
exempt-quota	Do not stop quota for these categories.	user	Not Specified	17
max-quota-timeout	Maximum FortiGuard quota used by single page view in seconds (excludes streams).	integer	Minimum value: 1 Maximum value: 86400	300
options	Options for FortiGuard Web Filter.	option	-	

Option	Description
error-allow	Allow web pages with a rating error to pass through.
rate-server-ip	Rate the server IP in addition to the domain name.
connect-request-bypass	Bypass connection which has CONNECT request.
ftgd-disable	Disable FortiGuard scanning.

Parameter	Description	Type	Size	Default
ovrd	Allow web filter profile overrides.	user	Not Specified	
rate-crl-urls	Enable/disable rating CRL by URL.	option	-	enable

Option	Description
disable	Disable rating CRL by URL.
enable	Enable rating CRL by URL.

rate-css-urls	Enable/disable rating CSS by URL.	option	-	enable

Option	Description
disable	Disable rating CSS by URL.
enable	Enable rating CSS by URL.

rate-javascript-urls	Enable/disable rating JavaScript by URL.	option	-	enable

Option	Description
disable	Disable rating JavaScript by URL.
enable	Enable rating JavaScript by URL.

config filters

Parameter	Description	Type	Size	Default
action	Action to take for matches.	option	-	monitor

Option	Description
block	Block access.
authenticate	Authenticate user before allowing access.
monitor	Allow access while logging the action.
warning	Allow access after warning the user.

auth-usr-grp <name>	Groups with permission to authenticate. User group name.	string	Maximum length: 79	
category	Categories and groups the filter examines.	integer	Minimum value: 0 Maximum value: 255	0

Parameter	Description	Type	Size	Default
id	ID number.	integer	Minimum value: 0 Maximum value: 255	0
log	Enable/disable logging.	option	-	enable

Option	Description
enable	Enable setting.
disable	Disable setting.

override-replacemsg	Override replacement message.	string	Maximum length: 28	
warn-duration	Duration of warnings.	user	Not Specified	5m
warning-duration-type	Re-display warning after closing browser or after a timeout.	option	-	timeout

Option	Description
session	After session ends.
timeout	After timeout occurs.

warning-prompt	Warning prompts in each category or each domain.	option	-	per-category

Option	Description
per-domain	Per-domain warnings.
per-category	Per-category warnings.

config quota

Parameter	Description	Type	Size	Default
category	FortiGuard categories to apply quota to (category action must be set to monitor).	user	Not Specified	
duration	Duration of quota.	user	Not Specified	5m
id	ID number.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
override-replacemsg	Override replacement message.	string	Maximum length: 28	
type	Quota type.	option	-	time

Option	Description
time	Use a time-based quota.
traffic	Use a traffic-based quota.

unit	Traffic quota unit of measurement.	option	-	MB

Option	Description
B	Quota in bytes.
KB	Quota in kilobytes.
MB	Quota in megabytes.
GB	Quota in gigabytes.

value	Traffic quota value.	integer	Minimum value: 1 Maximum value: 4294967295	1024

config override

Parameter	Description	Type	Size	Default
ovrd-cookie	Allow/deny browser-based (cookie) overrides.	option	-	deny

Option	Description
allow	Allow browser-based (cookie) override.
deny	Deny browser-based (cookie) override.

ovrd-dur	Override duration.	user	Not Specified	15m
ovrd-dur-mode	Override duration mode.	option	-	constant

Option	Description
constant	Constant mode.
ask	Prompt for duration when initiating an override.

Parameter	Description	Type	Size	Default
ovrd-scope	Override scope.	option	-	user

Option	Description
user	Override for the user.
user-group	Override for the user's group.
ip	Override for the initiating IP.
browser	Create browser-based (cookie) override.
ask	Prompt for scope when initiating an override.

ovrd-user-group `<name>`	User groups with permission to use the override. User group name.	string	Maximum length: 79	
profile `<name>`	Web filter profile with permission to create overrides. Web profile.	string	Maximum length: 79	
profile-attribute	Profile attribute to retrieve from the RADIUS server.	option	-	Login-LAT-Service

Option	Description
User-Name	Use this attribute.
NAS-IP-Address	Use this attribute.
Framed-IP-Address	Use this attribute.
Framed-IP-Netmask	Use this attribute.
Filter-Id	Use this attribute.
Login-IP-Host	Use this attribute.
Reply-Message	Use this attribute.
Callback-Number	Use this attribute.
Callback-Id	Use this attribute.
Framed-Route	Use this attribute.
Framed-IPX-Network	Use this attribute.
Class	Use this attribute.
Called-Station-Id	Use this attribute.

Parameter	Description	Type	Size	Default
	Option / **Description** *Calling-Station-Id* — Use this attribute. *NAS-Identifier* — Use this attribute. *Proxy-State* — Use this attribute. *Login-LAT-Service* — Use this attribute. *Login-LAT-Node* — Use this attribute. *Login-LAT-Group* — Use this attribute. *Framed-AppleTalk-Zone* — Use this attribute. *Acct-Session-Id* — Use this attribute. *Acct-Multi-Session-Id* — Use this attribute.			
profile-type	Override profile type. **Option** / **Description** *list* — Profile chosen from list. *radius* — Profile determined by RADIUS server.	option	-	list

config web

Parameter	Description	Type	Size	Default
bword-table	Banned word table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
bword-threshold	Banned word score threshold.	integer	Minimum value: 0 Maximum value: 2147483647	10

Parameter	Description	Type	Size	Default
content-header-list	Content header list.	integer	Minimum value: 0 Maximum value: 4294967295	0
urlfilter-table	URL filter table ID.	integer	Minimum value: 0 Maximum value: 4294967295	0

config webfilter search-engine

Configure web filter search engines.

Syntax

```
config webfilter search-engine
    edit <name>
        set charset [utf-8|gb2312]
        set hostname {string}
        set query {string}
        set safesearch [disable|url|...]
        set safesearch-str {string}
        set url {string}
    next
end
```

config webfilter search-engine

Parameter	Description	Type	Size	Default
charset	Search engine charset.	option	-	utf-8
	Option / **Description** *utf-8* — UTF-8 encoding. *gb2312* — GB2312 encoding.			
hostname	Hostname (regular expression).	string	Maximum length: 127	
name	Search engine name.	string	Maximum length: 35	
query	Code used to prefix a query (must end with an equals character).	string	Maximum length: 15	

Parameter	Description	Type	Size	Default
safesearch	Safe search method. You can disable safe search, add the safe search string to URLs, or insert a safe search header.	option	-	disable

Option	Description
disable	Site does not support safe search.
url	Safe search selected with a parameter in the URL.
header	Safe search selected by search header (i.e. youtube.edu).

safesearch-str	Safe search parameter used in the URL.	string	Maximum length: 79
url	URL (regular expression).	string	Maximum length: 127

config webfilter urlfilter

Configure URL filter lists.

Syntax

```
config webfilter urlfilter
    edit <id>
        set comment {var-string}
        config entries
            Description: URL filter entries.
            edit <id>
                set action [exempt|block|...]
                set antiphish-action [block|log]
                set dns-address-family [ipv4|ipv6|...]
                set exempt {option1}, {option2}, ...
                set referrer-host {string}
                set status [enable|disable]
                set type [simple|regex|...]
                set url {string}
                set web-proxy-profile {string}
            next
        end
        set ip-addr-block [enable|disable]
        set name {string}
        set one-arm-ips-urlfilter [enable|disable]
    next
end
```

Parameters

Parameter	Description	Type	Size	Default
comment	Optional comments.	var-string	Maximum length: 255	
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
ip-addr-block	Enable/disable blocking URLs when the hostname appears as an IP address.	option	-	disable

Option	Description
enable	Enable blocking URLs when the hostname appears as an IP address.
disable	Disable blocking URLs when the hostname appears as an IP address.

Parameter	Description	Type	Size	Default
name	Name of URL filter list.	string	Maximum length: 63	
one-arm-ips-urlfilter	Enable/disable DNS resolver for one-arm IPS URL filter operation.	option	-	disable

Option	Description
enable	Enable DNS resolver for one-arm IPS URL filter operation.
disable	Disable DNS resolver for one-arm IPS URL filter operation.

config entries

Parameter	Description	Type	Size	Default
action	Action to take for URL filter matches.	option	-	exempt

Option	Description
exempt	Exempt matches.
block	Block matches.
allow	Allow matches (no log).
monitor	Allow matches (with log).

Parameter	Description	Type	Size	Default
antiphish-action	Action to take for AntiPhishing matches.	option	-	block

Parameter	Description	Type	Size	Default
	Option / **Description** *block* — Block matches. *log* — Allow matches with log.			
dns-address-family	Resolve IPv4 address, IPv6 address, or both from DNS server.	option	-	ipv4
	Option / **Description** *ipv4* — Resolve IPv4 address from DNS server. *ipv6* — Resolve IPv6 address from DNS server. *both* — Resolve both IPv4 and IPv6 addresses from DNS server.			
exempt	If action is set to exempt, select the security profile operations that exempt URLs skip. Separate multiple options with a space.	option	-	av web-content activex-java-cookie dlp fortiguard range-block antiphish all
	Option / **Description** *av* — AntiVirus scanning. *web-content* — Web filter content matching. *activex-java-cookie* — ActiveX, Java, and cookie filtering. *dlp* — DLP scanning. *fortiguard* — FortiGuard web filtering. *range-block* — Range block feature. *pass* — Pass single connection from all. *antiphish* — AntiPhish credential checking. *all* — Exempt from all security profiles.			
id	Id.	integer	Minimum value: 0 Maximum value: 4294967295	0

Parameter	Description	Type	Size	Default
referrer-host	Referrer host name.	string	Maximum length: 255	
status	Enable/disable this URL filter.	option	-	enable
	Option / **Description** *enable* — Enable this URL filter. *disable* — Disable this URL filter.			
type	Filter type (simple, regex, or wildcard).	option	-	simple
	Option / **Description** *simple* — Simple URL string. *regex* — Regular expression URL string. *wildcard* — Wildcard URL string.			
url	URL to be filtered.	string	Maximum length: 511	
web-proxy-profile	Web proxy profile.	string	Maximum length: 63	

diagnose

Use `diagnose` commands to view and debug system information.

- diagnose autoupdate versions on page 206
- diagnose debug on page 207
- diagnose sniffer packet on page 208
- diagnose sys on page 208
- diagnose test application on page 210

diagnose autoupdate versions

Dump database and engine versions.

For each database, this command displays the database version as well as the time and result of the last update attempt, if applicable.

```
diagnose autoupdate versions
```

diagnose debug

Enable or disable debugging and view debugging configuration.

diagnose debug application

Set or view debugging levels for each application.

```
diagnose debug application <application> [debug level]
```

diagnose debug application

Parameter	Description	Type	Size	Default
application	Application name	string	-	
	Option / **Description** *certd* — Debug certd. *httpd* — Debug httpd. *iked* — Debug iked. *ipsengine* — Debug ipsengine. *ipsmonitor* — Debug ipsmonitor. *miglogd* — Debug miglogd. *restapi* — Debug the REST API. *syslogd* — Debug syslogs. *urlfilter* — Debug urlfilter.			

debug level	Set the debug level.
	Each application has different debug levels available.
	To see the available levels and the current setting, enter the command without the `debug level` value.
	For example, `diagnose debug application iked` displays:
	`ike debug level is 0`
	`info, 4: debug`
		string	-	`3:`

diagnose debug disable

Disable debugging.

```
diagnose debug disable
```

diagnose debug enable

Enable debugging.

```
diagnose debug enable
```

diagnose sniffer packet

Run a packet sniffer to view network traffic.

```
diag sniffer packet [<interface> <filter> <verbose> <count> <tsformat> <frame size>]
```

diagnose sniffer packet

Parameter	Description	Type	Size	Default
interface	Network interface to sniff (or "any").	string	-	any
filter	Flexible logical filters for sniffer (or "none"). For example: To print UDP 1812 traffic between forti1 and either forti2 or forti3: `udp and port 1812 and host forti1 and ( forti2 or forti3 )`	string	-	
verbose	• `1`: Print header of packets. • `2`: Print header and data from IP of packets. • `3`: Print header and data from ethernet of packets (if available). • `4`: Print header of packets with interface name. • `5`: Print header and data from IP of packets with interface name. • `6`: Print header and data from ethernet of packets (if available) with interface name.	integer	Minimum value: 1 Maximum value: 6	1
count	Sniffer count.	integer		
tsformat	Format of timestamp. • `a`: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms • `l`: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms • otherwise: relative to the start of sniffing, ss.ms	string		
frame size	Set the frame size that is printed before truncation. Defaults to the interface MTU.			

diagnose sys

View system information.

- diagnose sys botnet-ip list on page 209
- diagnose sys license on page 209
- diagnose sys status on page 209
- diagnose sys top on page 209

diagnose sys botnet-ip list

List known botnets.

```
diagnose sys botnet-ip list
```

diagnose sys license

Show license information.

```
diagnose sys license
```

diagnose sys license

Field	Description
Status	The license status.
SN	The device serial number.
Valid From	The license start date.
Valid To	The license expiration date.

diagnose sys status

Show system status.

```
diagnose sys status
```

diagnose sys status

Field	Description
Version	The Container FortiOS version and build number.
Serial-Number	The device serial number.
System time	The current system time, with timezone.

diagnose sys top

Show top processes information.

```
diagnose sys top
```

This command is similar to the standard Linux `top` command, with a limited set of interactions available. The set of columns displayed is not editable.

By default, the table is sorted by `%CPU`.

The following interactive commands are available:

Command	Description
`S | s`	Turn on cumulative time mode. Each process is listed with the CPU time it and its children have used.
`1 | C | c`	Toggle CPU single or separate display in the summary area.
`M | m`	Sort by `%MEM` (memory usage) column, which is not displayed.
`N | n`	Sort by `PID` (process ID) column.
`P | p`	Sort by `%CPU` (CPU usage) column.
`R | r`	Reverse the order of the current sort.
Up, PgUp, down, PgDn	Scroll up or down through the list.
Home, End	Scroll to the top of bottom of the list.

diagnose test application

Test, view information about, and perform operations on system applications.

```
diagnose test application <application> [option]
```

diagnose test application

Parameter	Description	Type	Size	Default
application	Application name	string	-	

Option	Description
ipsmonitor	Display information about the IPS engine and perform operations.
miglogd	View local log daemon information.
syslogd	View syslogd daemon information.
restapi	Test access to the REST API.

ipsmonitor

Parameter	Description	Type	Size	Default
option	The information to display or operation to perform.	integer	-	

Parameter	Description	Type	Size	Default
	Option / **Description** 1 / Display IPS engine information. 2 / Toggle IPS engine enable/disable status. 3 / Display restart log. 4 / Clear restart log. 5 / Toggle bypass status. 6 / Submit attack characteristics now. 10 / IPS queue length. 11 / Clear IPS queue length. 12 / IPS L7 socket statistics. 13 / IPS session list. 14 / IPS NTurbo statistics. 15 / IPSA statistics. 18 / Display session info cache. 19 / Clear session info cache. 21 / Reload FSA malicious URL database. 22 / Reload allowlist URL database. 24 / Display Flow AV statistics. 25 / Reset Flow AV statistics. 32 / Reload certificate blocklist database. 40 / Display packet log statistics. 41 / Reset packet log statistics. 96 / Toggle IPS engines watchdog timer. 97 / Start all IPS engines. 98 / Stop all IPS engines. 99 / Restart all IPS engines and monitor.			

miglod

Parameter	Description	Type	Size	Default
option	The information to display or operation to perform.	integer	-	

Parameter	Description	Type	Size	Default
	Option **Description** 4 Show log statistics. 16 Show log disk usage. 48 Show publish info.			

syslogd

Parameter	Description	Type	Size	Default
option	The information to display or operation to perform.	integer	-	
	Option **Description** 1 Show syslog setting. 3 Show syslog statistics 5 Show dropped logs due to log rate limit for all devices. 6 Show subscribe log info 7 Show subscribe log filter 9 Show remote sockets.			

restapi

Parameter	Description	Type	Size	Default
host	The REST API host address.	ipv4-address or FQDN	-	
port	The REST API host listening port.	integer	-	

execute

Execute static commands.

Syntax

```
execute {
    api-user generate-key <name>
    config backup <filename> [password] |
```

```
    import-vmlicense <license_string> |
    log filter category <category> |
    log filter device <device> |
    log filter dump |
    log display |
    log delete |
    log delete-all |
    ping <host> |
    shutdown |
    telnet <host> [port] |
    update-now |
}
```

Commands

Command	Description
config backup	Back up full configuration to `<filename>` in the `/data` directory. If `password` is specified, the backup config file will be encrypted with it.
import-vmlicense	Import license. Paste the full contents of the license file, enclosed in quotes.
log filter category	Specify the log category to filter on for `display` or `delete`. Press `Enter` without entering a category to see a list of available categories.
log filter device	Specify the log category to filter on for `display` or `delete`. Press `Enter` without entering a device to see a list of available devices.
log filter dump	Display the currently set log filters.
log display	Display the logs matching the currently set log filters.
log delete	Delete the logs matching the currently set log filters.
log delete-all	Delete all logs.
ping	Ping remote hosts. `host` may be an IP address or fully qualified domain name.
shutdown	Shutdown system immediately.
telnet	Connect to `host` using a simple telnet client.
update-now	Update FortiGuard definitions.

exit

Exit the CLI.

`exit` can only be used at the root level of the CLI.

Usage

```
exit
```

get

Use `get` to display dynamic and system information.

The syntax and options for `get` are usually the same as `config`.

For example, `get firewall address` displays a result similar to the following:

```
== [ FABRIC_DEVICE ]
name: FABRIC_DEVICE
== [ all ]
name: all
== [ login.microsoft.com ]
name: login.microsoft.com
== [ login.microsoftonline.com ]
name: login.microsoftonline.com
== [ login.windows.net ]
name: login.windows.net
== [ none ]
name: none
== [ wildcard.dropbox.com ]
name: wildcard.dropbox.com
== [ wildcard.google.com ]
name: wildcard.google.com
```

For available options, see config on page 15.

show

The show command displays the specified system configuration.

The syntax and options for `show` are the same as `config`.

For example, `show firewall address` displays a result similar to the following:

```
config firewall address
    edit "FABRIC_DEVICE"
        set comment "IPv4 addresses of Fabric Devices."
    next
    edit "all"
    next
    edit "login.microsoft.com"
        set type fqdn
        set fqdn "login.microsoft.com"
    next
    edit "login.microsoftonline.com"
        set type fqdn
```

```
        set fqdn "login.microsoftonline.com"
    next
    edit "login.windows.net"
        set type fqdn
        set fqdn "login.windows.net"
    next
    edit "none"
        set subnet 0.0.0.0 255.255.255.255
    next
    edit "wildcard.dropbox.com"
        set type fqdn
        set fqdn "*.dropbox.com"
    next
    edit "wildcard.google.com"
        set type fqdn
        set fqdn "*.google.com"
    next
end
```

For available options, see config on page 15.

sysctl sh

Enter the Linux shell.

Container FortiOS allows access the Linux shell.

```
sysctl sh
```

To return to or start the Container FortiOSshell, enter `/bin/cli` at the shell prompt.

www.fortinet.com