

Upgrade Guide for FortiOS 2.80

FORTINET™

www.fortinet.com

Upgrade Guide for FortiOS 2.80
29 August 2006
01-28000-0337-20060829

© Copyright 2006 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Contents

Introduction	9
About this document.....	9
Document conventions.....	9
Typographic conventions.....	10
Fortinet documentation	10
Fortinet documentation CD	11
Fortinet Knowledge Center	11
Comments on Fortinet technical documentation	11
Customer service and technical support	12
Upgrade Notes.....	13
Backing up configuration files	13
LCD display changes	13
Web-based manager changes	14
Viewing system status	14
System status	15
Unit Information	15
Recent Virus Detections	15
Content Summary.....	15
Interface Status.....	15
System Resources.....	16
History.....	16
Recent Intrusion Detections.....	16
Changes to the web-based manager	17
Command Line Interface changes	17
Icons in FortiOS 2.80.....	18
Other	19
New features and changes.....	29
CLI command changes	30
System.....	30
Status	31
Sessions.....	31
Network	31
DHCP	31
Service.....	32
Server	32
Exclude Range	32
IP/Mac Binding.....	32

Dynamic IP	32
Config.....	32
Admin.....	33
Maintenance	34
Virtual Domain	35
Router	36
Static.....	36
Policy	36
RIP	37
General.....	37
Networks.....	37
Interface.....	37
Distribution List.....	37
Offset List	37
Router Objects	38
Access List	38
Prefix List.....	38
Route-map.....	38
Key-chain.....	38
Monitor	39
Firewall	39
User.....	39
VPN	39
IPSec	39
PPTP.....	40
IPS.....	40
Signature.....	40
Anomaly	41
Antivirus	41
File Block	41
Config.....	42
Web Filter	42
URL Block	42
Category Block.....	43
Script Filter	43
Spam Filter	43
FortiGuard-AntiSpam	44
IP Address	44
DNSBL and ORDBL.....	44
Email Address.....	45
MIME Headers	45
Banned Word	45

Log & Report	46
Log Config.....	46
Log Settings.....	46
Log Filter.....	47
Log Access.....	48
HA	48
Using Perl regular expression in FortiOS 2.80	49
New features and changes for FortiOS 2.80MR8 to FortiOS 2.80MR10	50
Alert Message Console	50
Unit Information.....	50
Preventing the public FortiGate interface from responding to ping requests	50
Access Profile for prof_admin	51
Subordinate units block multicast and broadcast traffic in HA	51
Subordinate units, logging and SNMP in HA	51
Updating MAC forwarding tables when a link failover occurs in HA	51
Command syntax.....	52
FortiManager configuration	52
FortiGate SNMP traps and fields	52
FortiGate MIB fields	54
Chassis status – FortiGate-5000.....	56
SMC.....	56
Node cards	57
Switch cards	57
Chassis status – FortiGate-4000.....	57
Chassis status	57
Blade status	58
Out of band management.....	59
Firewall.....	59
VPN.....	59
Updates to Phase 1 Peer Options documentation.....	59
Phase 1 Peer ID used in dynamic DNS configurations	60
Destination IP address for FortiClient dialup clients	60
VIP Addresses for the FortiClient dialup clients.....	61
Dialup server mode of operation.....	61
Support for FortiGate dialup clients	61
IPS	62
system autoupdate ips.....	63
system global ips-open	63
system global ip_siganture	63
system global ips-size.....	63
Antivirus	63
system global av_failopen	63

system global optimize	64
Web Filter.....	64
Spam Filter.....	64
New features and changes for FortiOS 2.80MR11.....	65
MTU Settings for VLAN subinterfaces	65
Chassis status for FortiGate-5001 and FortiGate-5001FA2	65
SMC.....	65
Node cards	65
Switch cards	65
FortiGate 5001 Blade configuration	66
Firewall.....	66
SMTP virus scanning only operates in splice mode	67
Spam filter email tagging for SMTP is not supported	67
SMTP quarantine file name system generated	67
The default mail virus replacement message (splice mode)	67
VPN Tunnel description update.....	68
Subnet specified for IP pool correction.....	68
Mark as clear Spam Action correction.....	68
System Interface CLI command: forward_domain	68
Firewall CLI Commands	69
SIP.....	70
IPSec VPN	70
Phase 1 advanced settings	72
Phase 2 advanced options	72
Dialup monitor	72
config vpn ipsec phase 1	73
config vpn ipsec phase 2	73
Spam Filter.....	74
Upgrading to FortiOS 2.80	75
Backing up your configuration	75
Backing up your configuration using the web-based manager.....	75
Backing up your configuration using the CLI	76
Backing up your replacement messages.....	76
Testing FortiOS 2.80 before installing it.....	76
Verify the test firmware.....	77
Upgrading your FortiGate unit	77
Upgrading to FortiOS 2.80	78
Upgrading using the web-based manager.....	78
Upgrading using the CLI.....	78
Verifying the upgrade.....	79
Converting your replacement messages to FortiOS 2.80.....	79
Upgrading to FortiOS 2.80 using the FortiManager System	80

Upgrading FortiOS 2.80 firmware releases	81
Upgrading using the web-based manager	82
Upgrading using the CLI	83
Install firmware from a system reboot using the CLI	84
Reverting to FortiOS 2.50	87
Backing up your FortiOS 2.80 configuration	87
Downgrading to FortiOS 2.50 using web-based manager	88
Verifying the downgrade	88
Downgrading to FortiOS 2.50 using the CLI	88
Restoring your configuration	89
Restoring your configuration settings using the web-based manager	89
Restoring your configuration settings using the CLI.....	90
Re-establishing connections.....	90
Re-establishing administrative access settings	90
Re-establishing Internet connection	91
Reverting to a previous FortiOS 2.80 firmware version.....	91
Reverting to a previous firmware version using the web-based manager .	91
Reverting to a previous firmware version using the CLI	92
Index.....	95

Introduction

FortiOS 2.80 is a more dynamic and robust operating system, offering you even better protection, blocking and monitoring features for your network.

The Upgrade Guide provides you with information on FortiOS 2.80, and addresses any issues that may arise concerning your current configuration. With these new features, and improvements to existing features, you need to know how they may or may not affect your current configuration. The guide provides you with information on backing up your current configuration, and installing FortiOS 2.80 on your FortiGate unit.

About this document

This document contains the following chapters:

- [Upgrade Notes](#) – Provides information on changes and new features for FortiOS 2.80 and all subsequent FortiOS 2.80 maintenance releases.
- [New features and changes](#) – Provides general information on what has changed from FortiOS 2.50MR10 to FortiOS 2.80MR11. Includes indepth information about new features and changes for FortiOS 2.80MR8 to FortiOS 2.80MR10, and FortiOS 2.80MR11.
- [Upgrading to FortiOS 2.80](#) – Describes how to install FortiOS 2.80, including addressing issues about FortiOS 2.80, backing up your current configuration settings, and verifying the upgrade installed successfully. Includes how to upgrade FortiOS 2.80 maintenance releases.
- [Reverting to FortiOS 2.50](#) – Describes how to downgrade your FortiGate unit to FortiOS 2.50, or a FortiOS 2.80 maintenance release, including how to restore your configuration settings for FortiOS 2.50.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:



Note: Highlights useful additional information.



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

Typographic conventions

FortiGate documentation uses the following typographical conventions:

Convention	Example
Keyboard input	In the Gateway Name field, type a name for the remote VPN peer or client (for example, <code>Central_Office_1</code>).
Code examples	<pre>config sys global set ips-open enable end</pre>
CLI command syntax	<pre>config firewall policy edit id_integer set http_retry_count <retry_integer> set natip <address_ipv4mask> end</pre>
Document names	<i>FortiGate Administration Guide</i>
Menu commands	Go to VPN > IPSEC > Phase 1 and select Create New.
Program output	Welcome!
Variables	<address_ipv4>

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following [FortiGate product documentation](#) is available:

- *FortiGate QuickStart Guide*
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Install Guide*
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.

- [FortiGate Log Message Reference](#)
Available exclusively from the [Fortinet Knowledge Center](#), the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- [FortiGate High Availability User Guide](#)
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- [FortiGate IPS User Guide](#)
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- [FortiGate IPSec VPN User Guide](#)
Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- [FortiGate SSL VPN User Guide](#)
Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- [FortiGate PPTP VPN User Guide](#)
Explains how to configure a PPTP VPN using the web-based manager.
- [FortiGate Certificate Management User Guide](#)
Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- [FortiGate VLANs and VDOMs User Guide](#)
Describes how to configure VLANs and VDOMs in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet documentation CD

All Fortinet documentation is available from the Fortinet documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Knowledge Technical Documentation web site at <http://docs.forticare.com>.

Fortinet Knowledge Center

The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

Comments on Fortinet technical documentation

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

Customer service and technical support

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

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

Upgrade Notes

FortiOS 2.80 includes many new features, including a redesigned web-based manager and CLI, along with changes to existing features. It is recommended you read this chapter before downloading FortiOS 2.80. By reading this chapter, you learn about the new features and/or changes to existing features for FortiOS 2.80. This chapter describes these changes and features to FortiOS 2.80.

It is recommended to also review the *FortiGate CLI Reference Guide* for the new and revised CLI commands as well as the *FortiGate Administration Guide* for your specific FortiGate unit.

This section includes the following:

- [Backing up configuration files](#)
- [LCD display changes](#)
- [Web-based manager changes](#)
- [Web-based manager changes](#)
- [Changes to the web-based manager](#)
- [Command Line Interface changes](#)
- [Other](#)

The following is general information about FortiOS 2.80. For information concerning FortiOS 2.80 maintenance releases, see [“Other” on page 19](#).



Note: Make sure you have the administration guide, installation guide (for your specific FortiGate unit(s)), and release notes before upgrading to FortiOS 2.80. You may require additional information than this Upgrade Guide provides after installing FortiOS 2.80.

Backing up configuration files

You now have the option to backup configuration files with or without a password for additional security. You can backup individual configuration files or all configuration files. Backing up these files is located in **System > Maintenance > Backup and Restore**. This location also restores these files.

LCD display changes

After upgrading to FortiOS 2.80, FortiGate units with an LCD screen will display the following main menu:

Figure 1: LCD main menu display in NAT/Route mode

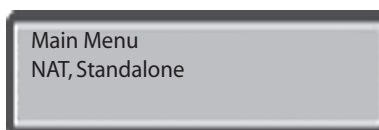
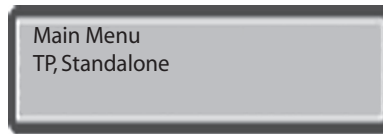


Figure 2: LCD main menu display in Transparent mode



Web-based manager changes

The system dashboard in FortiOS 2.80 has been redesigned, along with various system information now categorized on the Status page. The set-up wizard has been redesigned for FortiOS 2.80 as well.



Note: Replacement messages in FortiOS 2.50 must be manually updated in FortiOS 2.80. See [“Backing up your replacement messages” on page 76](#) and [“Converting your replacement messages to FortiOS 2.80” on page 79](#) for more information.

Figure 3: System Dashboard of a FortiGate-400

The screenshot shows the FortiGate-400 WEB CONFIG interface. The left sidebar contains navigation options: System, Router, Firewall, User, VPN, IPS, Anti-Virus, Web Filter, Spam Filter, and Log&Report. The main content area is divided into several sections:

- Alert Message Console:** Shows system restart logs for 2006-03-27.
- System Status:**
 - Uptime: 1 day(s) 0 hour(s) 23 min(s)
 - System Time: Tue Mar 28 05:53:38 2006
 - Log Disk: Not available
 - Notification: [Change Password](#) [Product Registration](#)
- Interface:**

Interface	IP/Netmask	Status
port1	172.20.120.140/255.255.255.0	Up
port2	192.168.100.99/255.255.255.0	Up
port3		Up
port4/ha		Up
- Unit Information:**
 - Host Name: FGT-400 [[Change](#)]
 - Firmware Version: Fortigate-400 2.80,build4489,051027 [[Update](#)]
 - FortiGuard - AV Definitions: 6,123(10/26/2005 14:55) [[Update](#)]
 - FortiGuard - Intrusion Definitions: 2,240(10/20/2005 17:01) [[Update](#)]
 - Serial Number: FGT4002803033479
 - Operation Mode: NAT [[change](#)]
- System Resources:**
 - CPU Usage: 0%
 - Memory Usage: 28%
 - Active Sessions: 2
 - Network Utilization: 2 kbps
- Recent Virus Detections:** No virus detected.
- Content Summary:** Since 03/27/2006 05:30:14 [[reset](#)].
 - HTTP: 0 URLs visited [[details](#)]
 - Email: 0 emails sent, 0 emails received [[details](#)]
 - FTP: 0 URLs visited, 0 files uploaded, 0 files downloaded [[details](#)]

At the bottom, there is an 'Automatic Refresh Interval' dropdown set to 'none' and a 'Refresh' button.

Viewing system status

- Automatic Refresh Interval** Select to control how often the web-based manager updates the system status display.
- Go** Select to set the selected automatic refresh interval.
- Refresh** Select to manually update the system status display.

System status

Uptime	The time in days, hours, and minutes since the FortiGate unit was last started.
System Time	The current time according to the FortiGate unit's internal clock.
Log Disk	Displays hard disk capacity and free disk space if the FortiGate unit contains a hard disk. If no hard disk is installed, Not Available displays.
Notification	Contains reminders such as "Change Password" or "Product Registration". Select the reminder to see the detailed reminder message.

Unit Information

Host Name	The host name of the current FortiGate unit.
Firmware Version	The current firmware version installed on the FortiGate unit.
Antivirus Definitions	The current installed version of the FortiGate Antivirus Definitions.
Attack Definitions	The current installed version of the FortiGate Attack Definitions used by the Intrusion Prevention System (IPS).
Serial Number	The serial number of the FortiGate unit. The serial number is specific to the FortiGate unit and does not change with firmware upgrade.
Operation Mode	The operation mode of the FortiGate unit.

Recent Virus Detections

Time	The time when the recent virus was detected.
Src/Dst	The source and destination addresses of the virus.
Service	The service where the virus was delivered: HTTP, FTP, IMAP, POP3, SMTP.
Virus Detected	The name of the virus detected.

Content Summary

Reset	Select to reset the count values in the table to zero.
HTTP	The number of URLs visited. Select Details to see the list of URLs, the time they were accessed and the IP address of the host that accessed them.
Email	The number of emails sent and received. Select Details to see the date and time, the sender, the recipient and the subject of each email.
FTP	The number of URLs visited, including the number of files uploaded and downloaded. Select Details to see the FTP site URL, date, time, user, including lists of files uploaded and downloaded.

Interface Status

Interface	The name of the interface.
IP/Netmask	The IP address and netmask of the interface (NAT/Route mode only).
Status	The status of the interface, either up (green up arrow) or down (red down arrow).

System Resources

CPU Usage	The current CPU status. The web-based manager displays CPU usage for core processes only. Management processes are excluded.
Memory Usage	The current memory status. The web-based manager displays memory usage for core processes only. Management processes are excluded.
Hard Disk Usage	The current hard disk (local disk) status. The web-based manager displays hard disk usage for core processes only. Management processes are excluded.
Active Sessions	The number of communication sessions being processed by the FortiGate unit.
Network Utilization	The total network bandwidth being used through all FortiGate interfaces and the percentage of the maximum network bandwidth that can be processed by the FortiGate unit.
History	Select History to view a graphical representation of the last minute of CPU, memory, sessions, and network usage. This page also shows the virus and intrusion detections over the last twenty hours.

History

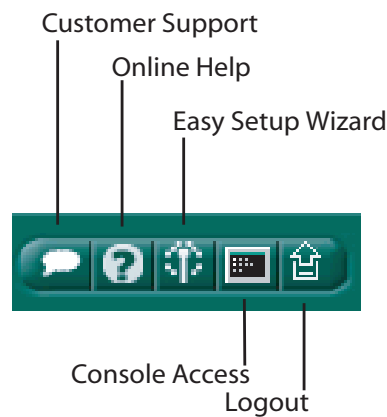
CPU Usage History	CPU usage for the previous minute.
Memory Usage History	Memory usage for the previous minute.
Session History	Session history for the previous minute.
Network Utilization History	Network utilization for the previous minute.
Virus History	The virus detection history over the last twenty hours.
Intrusion History	The intrusion detection history over the last twenty hours.

Recent Intrusion Detections

Time	The time when the recent intrusion was detected.
Src/Dst	The source and destination addresses of the attack.
Service	The service where the attack was delivered: HTTP, FTP, IMAP, POP3, or SMTP.
Attack Name	The name of the attack.

The following shows the new button bar icons in the top right corner of the web-based manager. These icons are always displayed and provide access to several important FortiGate features.

Figure 4: Button bar icons located in the top right corner of the web-based manager



- Contact Customer Support – For a first-time user to register their FortiGate unit.
- Online Help – Provides you with web-based help for the current web-based manager page, and hyperlinks take you to related topics and procedures related to the controls on the current page.
- Easy Setup Wizard – Provides a quick and easy way for first-time users to configure initial settings for the FortiGate unit.
- Console Access – Provides you with access to the CLI through the web-based manager. Since this is a Java-based terminal application, you must have a management computer with Java version 1.3 or higher installed.
- Logout – Immediately logs you out of the web-based manager.

Changes to the web-based manager

In FortiOS 2.80, the web-based manager has been redesigned and additional features added. See the [“New features and changes” on page 29](#) for more information.

If you need additional information on these new features, see your *FortiGate Administration Guide* for your specific FortiGate unit for more information.

Command Line Interface changes

In FortiOS 2.80, the Command Line Interface (CLI) command structure has been restructured and new commands added. It is recommended you review the *FortiGate CLI Reference Guide* to familiarize yourself with the restructure command hierarchy and the new commands for FortiOS 2.80.

See the *FortiGate CLI Reference Guide* for more information

Icons in FortiOS 2.80

The following tables display the new icons for FortiOS 2.80, along with any icons that have changed from FortiOS 2.50. In FortiOS 2.80, you can move your mouse over an icon to view the tooltip for that icon.

Table 1: FortiOS 2.50 icons that changed in FortiOS 2.80


























Icon v2.50	Icon v.280	Name	Description
		Edit	Edit a configuration. This icon appears in lists where you have write permission on the page.
		Delete	Deletes an item. This icon appears in lists where the item is deleteable and you have write permission on the page.
		Change Password	The change password icon is now available on the Admin page.
		Page Up/Previous Page	View the previous page of the list.
		Page Down/Next Page	View the next page of the list.
		Clear all/Clear	Clears a log file.
		Go	Do a search.
		Insert Policy Before	Inserts a firewall policy either before or after another firewall policy.
		Internal/External/Ports are up	Displays the connection status of each interface. The green up arrow indicates the interface is connected. You can select Bring Down next to the green up arrow to bring down an interface.
		Internal/External/Ports are down	Displays the connection status of each interface. The red down arrow indicates the interface is down or the interface is not connected. You can select Bring Up next to the red down arrow to bring up or connect an interface.

Table 2: New icons for FortiOS 2.80

Icon v.280	Name	Description
	Column settings	Select to display certain fields on each tab. For example, you can add from the Available fields list Status, Reason, and Type so these three fields display on the page along with the other fields. You can also move the fields either up or down in the Show these fields in this order list.
	Restore	Select to restore a configuration file.
	Move to	Select to move a setting either above or below another setting.
	Reset to	Resets all settings or a specific setting on the page to default settings.
	Backup	Select to backup your configuration file(s).


When you select the blue triangle icon , you reveal hidden options.

Figure 5: Hidden options for Traffic log, located on the Log Filter page

Other

The following are other issues concerning FortiOS 2.80 maintenance releases, from FortiOS 2.80MR4 to FortiOS 2.80MR11. If you are upgrading from FortiOS 2.80MR4 or earlier to FortiOS 2.80MR5 or later, it is recommended to read the following because these issues are not included in the above sections or in [“New features and changes” on page 29](#).

FortiOS 2.80MR12 is not included because this particular release of FortiOS 2.80 has the same issues as FortiOS 2.80MR11. Resolved issues are not included in this document. If you want to know the resolved issues for a particular maintenance release, see the Resolved Issues section of the Release Notes for that maintenance release.

These issues are carried forward from FortiOS 2.80MR4 to FortiOS 2.80MR11 unless otherwise stated. These issues are in descending order from FortiOS 2.80MR11 to FortiOS 2.80MR4.

Other Issues for FortiOS 2.80MR11

- The following default actions are changed in NIDS signatures later than version 2.214:
 - icmp_flood (clear_session => disable)
 - ping_death (drop => disable)
 - large_icmp (none => disable)
 - udp_flood (drop_session => disable)

- The system daylight savings mode must be configured before the timezone and current time is set because correct time is influenced by time zone and daylight savings mode.
- FastStart/H.245 Tunneling and Microsoft NetMeeting is supported in FortiOS 2.80MR11.
- The system configuration file created in **Maintenance > Backup & Restore > System Configuration** cannot store CA Certificates, Spam Filter and Web Filter settings. Backup these settings before upgrading to a current version of FortiOS 2.80. After upgrading, restore these settings before restoring the system configuration file.
- The Log policy, Local and Console setting found in FortiOS 2.50 is not supported in FortiOS 2.80MR11.
- The FortiGate firewall blades previously known as FortiBoost, are now known as FG5002FB2. Image names that begin with FGT_Boost are for the FG5002FB2 blades. Image names that begin with FGT_5000 are for the FG5001 blades.
- File blocking for file names encoded in the following character sets is no longer supported:
 - X-SJIF for Japanese characters
 - GB231 for Simplified Chinese characters
 - BIG5 for Traditional Chinese characters
 - EUC-KR for Korean characters
- Filenames that contain the following character sets are renamed to question marks in the replacement message:
 - X-SJIF for Japanese characters
 - GB231 for Simplified Chinese characters
 - BIG5 for Traditional Chinese characters
 - EUC-KR for Korean characters
- When specifying banned words with wildcard type, only the following are allowed:
 - a-z
 - A-Z
 - 0-9
 - \ ^ \$. [] | () { } + ? *

If you want to use other characters to specify a banned word, use regular expression type.

- Replacement message sizes are now 4096 bytes.
- FTP splice can now be disabled or enabled.
- All sessions are dropped when a unit with master override reboots and rejoins the HA cluster. This behavior appears only when the primary unit is rebooted or powered up, not when the interface is disconnected and reconnected.
- When an active link fails on the primary unit (Active-Active) cluster FortiGate firewall, all routes on the new subordinate unit are lost and are not relearned once the route-ttl time expires. This only affects networks where dynamic routing is used. You can set the route-ttl value to zero on the primary unit's FortiGate firewall.
- A dialup IPsec tunnel with a Phase 2 tunnel containing an underscore character is dropped whenever a firewall policy setting is changed.
- When a dialup VPN connection is made to a FortiGate firewall, the phase2 SA's timer is not reset automatically when there is still an active session. Enable the Phase 2 keepalive on the VPN dialup client to resolve this.
- The FortiGate firewall assigns reserved IP addresses to requesting DHCP clients when the FortiGate firewall non-reserved IP pool is used up.
- The Chassis option displays in the System menu even though this option is only supported on the FortiGate-5002 blade.

- Japanese characters in filenames are not blocked by the FortiGate firewall.
- The FortiGate firewall sends a replacement message when an infected file has Japanese characters in the filename. It replaces the name of the file with a series of question marks.

Other Issues for FortiOS 2.80MR10

- Fortinet's subscription-based services are now referred to as:
 - FortiGuard Antivirus
 - FortiGuard Intrusion Protection
 - FortiGuard AntiSpam
 - FortiGuard Web Filtering
- When a new IPS signature database is pushed to FortiGate by the FDS, IPS settings altered from their default values are overwritten. FortiOS 2.80MR10 introduces a new command to do one of two things. If the option is disabled, existing settings are not overwritten on updates received from the FDS. If the option is enabled, the default setting, the new IPS signature database is pushed with Fortinet recommended settings. The following is the new CLI command syntax:
 - ```
config system autoupdate ips
 set accept-recommended-settings {disable | enable}
end
```

This command can be used to prevent IPS signatures from being overwritten by future IPS signature updates.

- The ability to disable SMTP splice is supported in FortiOS 2.80MR10, when AV scanning is enabled. SMTP splice is enabled by default when AV scanning is enabled in the firewall policy, but can be turned off through the CLI. Administrators can choose between AV scanning or spam filter tagging of SMTP traffic since the AV splice operation now precludes the use of tagging an email message with a spam subject-line tag. Splice means the FortiGate Antivirus Firewall sends part of the message or file to the destination address while performing AV scanning.
- NetMeeting is supported in FortiOS 2.80MR10; however, FastStart and H.245 tunneling are not.

- The default settings of some IPS signatures were changed in IPS database version 2.211. If your firewall is using an IPS database version older than 2.211 and you upgrade to MR10 that has an IP database version 2.216, then the following signatures will change. You must manually change them if you want to enable them. Use the following CLI command to prevent these settings from being overwritten by future IPS signature updates.

```
config system autoupdate ips
 set accept-recommended-settings {disable | enable}
end
```

The following is a list of the signatures that changed.

- Signatures disabled by default:

```
CyberKit.2.2
SMB.DCERPC.SamrEnumerateAliasInDomain.139
Private.Access.UDP
ip_decoder:ipv4_bad_checksum
dns_decoder:invalid_pointer
dns_decoder:invalid_opcode
dns_decoder:invalid_param
CyberKit.2.2
SMB.DCERPC.SamrEnumerateAliasesInDomain.139
http_decoder:double_encoding
tcp_decoder:tcp_bad_checksum
im:aim
im:msn
im:yahoo
im:qq
pop_decoder:nested_request
pop_decoder:unknown_cmd
pop_decoder:unknown_reply
smtp_decoder:nested_request
smtp_decoder:unknown_cmb
smtp_decoder:unknown_reply
imap_decoder:unknown_cmd
imap_decoder:unknown_reply
udp_decoder:udp_bad_checksum
Private.Access.UDP
```

- Anomalies that changed:

```
icmp_src_session (100 => 200)
tcp_src_session (2000 => 5000)
udp_src_session (1000 => 5000)
```

- The **P2P > skype** IPS signature found in the web-based manager under **IPS > Signature > Predefined > p2p > skype** does not block Skype IM sessions when the action is set to “drop session” or “clear session”.
- If a DHCP relay agent is configured on the HA interface, DHCP DISCOVER messages are not forwarded to the DHCP server.
- When a FortiGate running RIPv2 has a passive interface, authentication enabled, and a neighbor configured, no authentication information is contained in any of the RIPv2 packets.
- Content logging may drop the first character of the From, To, and Subject header fields if they contain no space after the colon (:) delimitor.
- Using a blank field in the Command Name identified field allows all users defined in a Windows Active Directory to be authenticated, regardless of their position within the AD structure. If the Common Name Identifier field in an LDAP user is left blank, upon upgrading from FortiOS 2.80MR9 to FortiOS 2.80MR10, the field is filled in with “cn”, that causes authentication attempts to fail if the above method is used.

### Other issues relating to FortiOS 2.80MR9

- Before FortiOS 2.80MR9 (build 393), when the firewall adjusts its clock for daylight savings, the update daemon would restart continually, preventing the firewall from receiving antivirus and IPS updates. By disabling the daylight savings time options in **System > Config > Time**, you can work around this. You can either adjust the clock manually to compensate for the one hour difference or use NTP and select a time zone one hour ahead of your own.
- Each static route entered in the firewall has an index when entered either through the web-based manager or through the CLI. The index is used as the priority of the static route – the lower index value has the higher preference. Changes to affect the priority of identical static routes are made through the CLI.
- When upgrading from a FortiOS 2.50 image to a FortiOS 2.80 pre-MR5 release to FortiOS 2.80MR11 from the web-based manager, a message is displayed “The system configuration will be set to default. All the original configuration will be lost...”. This message is incorrect and clicking “OK” will not erase the current configuration. Previous versions of FortiOS do not handle the embedded RSA signature in the FortiOS 2.80MR9 image and cause of the display of this message.
- If your network carries H.323 traffic, Fortinet advises to keep FortiOS 2.80MR4 installed and not upgrade to FortiOS 2.80MR9. While FortiOS 2.80M9 resolved failing P2P call setups, there are issues present with Microsoft NetMeetings, FastStart, and H.245 tunneling.
- For FortiGate-300 units and above, static NAT VIPs are added after upgrading to FortiOS 2.80MR9 do not work until the configuration is re-written. For example,
  - configure static NAT VIP
  - add to firewall policy
  - re-apply any existing setting in the current configuration, such as a firewall address.VIPs that already exist prior to upgrade are not affected.
- The firewall does not block MSN Messenger and Yahoo! IM traffic when the protection profile is set to block IM and when firewall authentication is enabled. If firewall authentication is disabled, MSN Messenger and Yahoo! IM traffic is blocked as expected.
- The firewall does not display connected dialup tunnels if there are more than 20 static tunnels.
- Using the web-based manager to delete an SNMP host in a community deletes the hosts below it. Use the CLI to delete an SNMP host in a community.
- In the Protection Profile, if the following combinations of options under Spam Filtering are enabled the firewall does not perform the return e-mail domain name check. These following three options work independently:
  - IP Address FortiSpamshield check and Return e-mail DNS check
  - RBL & ORDBL check and Return e-mail DNS check
- Changes made to IPS signatures are not saved when restoring the configuration file or during an upgrade. For example, changes are not saved if you change the action on the “AskSam.as\_web.Access” signature in the iss group from Pass to Drop Session, then backup the configuration, upgrade the firewall, and then restore configuration.

### Other issues relating to FortiOS 2.80MR8

- FTP splice is now permanently enabled. SMTP splice is enabled when AV scanning is enabled in the affecting firewall policy. Administrators can choose between AV scanning or spam filter tagging of SMTP now that AV splice operation precludes the use of tagging an email message with a spam subject-line tag.  
Splice means the FortiGate Antivirus Firewall sends part of the message or file to the destined address while it performs AV scanning.
- Blocked connections to a non-standard HTTP port when FortiGuard functionality is enabled is no longer an issue.
- The “#” character in modem configuration strings is no longer an issue.
- In a HA cluster configuration, certain MIB OID location sometimes do not respond to SNMP GET queries, such as memory, cpu, and sessions. View this particular information from the web-based manager or CLI.
- To prevent XSS (cross site scripting) vulnerabilities, certain characters are disallowed in most CLI and web-based manager fields. The Web Pattern Block field currently does not allow the following characters:  
< > ( ) # “ ‘

### Other issues relating to FortiOS 2.80MR7

- Fortinet advises not to upgrade to FortiOS 2.80MR7 if your network carries H.323 traffic. While FortiOS 2.80MR7 permits H.323 connection set-up, unfortunately H.323 data traffic is blocked.
- Connections to a non-standard HTTP port, for example when using a web proxy, is blocked when FortiGuard functionality is enabled. Contact Fortinet Customer Support for assistance with this issue.
- The “#” character is not allowed in the modem configuration strings in FortiOS 2.80MR7. This could affect installations that use certain PBX devices or certain AT commands containing the “#” character. Contact Fortinet Customer Support for assistance with this issue.
- In HA cluster of three or more units running Active-Active with round-robin load distribution, if a node in the cluster enters “linkfail” status, the cluster unit sessions fail-over properly. When the node “linkfail” is resolved, or reconnected, it will not rejoin the cluster without issuing the “exec ha sync” CLI command from the HA primary unit. This only concerns the FortiGate-300A.
- When adding a new member to a HA cluster, the normal operation involves synchronizing the unit configuration followed by a system reboot of the new member. If the synchronization fails, the subordinate will continuously reboot as it repeatedly attempts to synchronize the configuration. This can occur if a configuration change is made on the primary unit when the HA link to the subordinate is down. Contact Customer Support for assistance.
- The IPSec Phase 2 single-source selector functions as expected when used to create a single tunnel for a dial-up client. It does not create a tunnel when used in a hub & spoke configuration with multiple dial-up clients.
- Use of a web proxy for HTTP traffic that directs client HTTP traffic to use a port other than TCP/80 will be blocked if FortiGuard functionality is enabled. Contact Fortinet Customer Support for assistance with this issue.

### Other issues relating to FortiOS 2.80MR6

- The entire FortiGate configuration settings in FortiOS 2.80MR5 and later are stored in a compressed format, called a zip format. These configuration settings are compressed in the zip format when you select All Configuration Files on the Backup & Restore page in the web-based manager.

- Antivirus scanning of oversize files or email messages (greater than 10MB or greater than 10 percent of system memory) requires temporary buffering to the internal hard disk on supported FortiGate units. This function is disabled and will be re-enabled in FortiOS 2.80MR5. Any files larger than the allowable AV scan memory limit are handed as indicated by the Protection Profile "Oversize file" setting. Ensure that all Protection Profiles have the AV Buffer-to-Disk option disabled prior to upgrading from pre-MR4 versions. Failure to do so will result in all AV scanning options disabled in all Protection Profiles after the upgrade.
- Firewall policies with incoming VIP interfaces that are PPPoE address assigned do not pass traffic.
- An alert email is not sent by the HA cluster for events occurring on a subordinate unit that would generate an alert email if the event occurred on the primary unit. Use a Syslog server to record the subordinate unit events.
- When joining a HA cluster, a new subordinate unit will not have the same configuration as the primary unit and therefore will respond with the "error" messages on the console. These messages are normal and the HA system will recover through a reboot of the new slave unit when synchronizing the new unit to the existing HA cluster configuration. This is intended behavior.
- Radius with MS-Chap v1 authentication will succeed, but the PPTP tunnel will not pass traffic. Other modes of authentication such as PAP, CHAP and MS-Chap v2 allow PPTP traffic to pass. Use MS-CHAP v2.
- The IPSec keylife does not expire when using a byte count value. Use a time value in seconds for keylife instead.
- Attempts to backup all configuration will fail if there is a pending certificate request. Complete certificate request prior to configuration backup.
- An interface down event sends the wrong SNMP trap. When an interface is unplugged and goes "DOWN" the SNMP trap for "UP" is sent. When in HA mode, multiple duplicate SNMP traps may be sent.
- On the FortiGate-100A and FortiGate-200A, static routes configured that use the internal 4-port interface do not show up on routing table, and some outgoing traffic may fail to pass through this port. Use an unused DMZ or WAN ports as the internal LAN network and construct policies and routes accordingly.

#### Other issues relating to FortiOS 2.80MR5

- When upgrading from a FortiOS 2.50 image to a FortiOS 2.80 pre-MR5 release to FortiOS 2.80MR11 from the web-based manager, a message is displayed "The system configuration will be set to default. All the original configuration will be lost...". This message is incorrect and clicking "OK" will not erase the current configuration. Previous versions of FortiOS do not handle the embedded RSA signature in the FortiOS 2.80MR5 image and cause of the display of this message.
- Access to the Content Log messages, HTTP, FTP, SMTP, POP3, IMAP content, is now through **Firewall > Protection Profile** settings and is only available through the FortiLog System settings. The IP address of the FortiLog System unit or a syslog unit can be configured to receive the Content Log messages. Content Log messages are no longer available on the Log Access page.
- Contact Fortinet Customer Support for assistance before upgrading to FortiOS 2.80 if your FortiGate configuration uses more than 10 Virtual Domains with Zones in Transparent mode operation because configuration settings may be lost.
- From the web-based manager, the spam filter lists "uncheck all" or "check all" does not take effect when enabling or disabling spam filter lists. You need to disable/enable list entries individually, or after a reboot the "disable/enable all" will take effect.

- The dial-up tunnel from a FortiClient endpoint in a concentrator configuration does not come up. Use “selectors from policy” in the FortiGate Phase 2 configuration and a specific FortiGate firewall policy from the hub network to the FortiClient VIP.
- All ‘source interface’ and ‘destination interface’ fields in traffic log messages become ‘n/a’. Contact Customer Support for an interim build.
- The Update Center in the web-based manager does not accept any changes. Click “Apply” or “Update Now” displays the error message “CFG\_CLI\_INTERNAL\_ERR”. Use the CLI commands to modify the Update Center settings:  
config system autoupdate <pushupdate/schedule>
- When accessing the IPS anomaly page using the web-based manager, the page display is very slow and could take 2-3 minutes to fully render. Repeated clicking on the Anomaly menu link increases the delay since each click is a new request to redraw the page.
- After less than 3 times of successful DHCP IP address renewals, the FortiGate DHCP client will stop sending a DHCP renew message. Change the interface mode to static and then change back to DHCP mode again.
- For FortiWiFi-60 units, the Modem interface can be set as a back-up should another interface fail. When WAN2 interface goes down the Modem interface does not automatically connect as the back-up connection.
- The following are SNMP traps that are not working in FortiOS 2.80MR5:
  - portscan
  - syn\_flood
  - virus detection
  - spu overusage
  - low memory
  - warm start
  - cold start
  - link up
  - link down
- The following are the only five types successfully generated:
  - interface ip change
  - management ip change
  - vpn tunnel up
  - vpn tunnel down
  - ha status change
 Contact Customer Support for an interim build.
- Executing a reset factory default does not clear the web pattern block settings of the previous configuration.

#### Other issues relating to FortiOS 2.80MR4

- When upgrading to FortiOS 2.80MR3, if a “File too big” error message is displayed, reboot the FortiGate firewall and attempt the upgrade again. The reboot will clear the internal RAM disk of the temporary files that may be blocking the upgrade process. If the condition still persists, backup all configuration files and use the flash memory reformat function from the console boot-up menu.
- Cerberian Web Filter functionality was removed in FortiOS 2.80MR3 and is no longer supported. This functionality is now provided by the FortiGuard-Web Filtering Service. Current Cerberian license holders are eligible for a free upgrade to the FortiGuard Web Filtering Services and should contact their local Fortinet Sales representative.

- Antivirus scanning of oversize files or email messages (greater than 10MB or greater than 10 percent of system memory) requires temporary buffering to the internal hard disk on supported FortiGate units. This function is disabled and will be re-enabled in FortiOS 2.80MR5. Any files larger than the allowable AV scan memory limit are handed as indicated by the Protection Profile "Oversize file" setting.
- Contact Customer Support for assistance if DynDNS IPSec tunnel functionality is required.
- Access to the Content Log messages (HTTP, FTP, SMTP, POP3, IMAP content) has been transferred to the FortiLog System to improve FortiGate system performance and off-load the system CPU. Content Log messages are no longer available from the web-based manager Log Access page.
- It is recommended when upgrading FortiGate-50A units from FortiOS 2.50 to FortiOS 2.80MR4 to following these procedures:
  - Upgrade to FortiOS 2.50MR10
  - For configuration settings, re-apply existing settings. For example, go to the Edit page for an address in firewall policies, and select OK to reapply the existing settings. This type of action forces an internal re-write of the configuration tables, ensuring they are preserved.
  - Upgrade to FortiOS 2.80MR4
- Contact Fortinet Technical Support for assistance before upgrading to 2.80 if your FortiGate configuration uses more than 10 Virtual Domains with Zones in Transparent mode operation. Configuration settings may be lost upon upgrading.
- When file over-size scanning is enabled to use the hard disk, the area on the hard disk may become corrupted which prevents further large files to be scanned or quarantined. On the FortiGate-1000, this problem is acute and may stop all AV scanning and block AV scannable traffic.
- With AV scanning enabled, when a POP3 mail message reaches the oversize file limit with the action set to "pass", the FortiGate firewall will send a NOOP command to the POP3 mail server while transferring the partial message to the client. The FortiGate attempts to resume the message download from the server, but the server has timed out and closed the connection.
- When Alert Mail is enabled and a virus is detected, the content of the message is always the standard syslog type message even if the replacement message is selected in the configuration. You can work around this problem using the CLI.
- If configured in an encrypt firewall policy, IPSec NAT-outbound does not translate the internal IP address as expected. Contact Customer Support for an interim solution.
- If governed by a NAT firewall policy, Oracle SQL\*NET data sessions will close prematurely when the control session is closed or times out.
- All sessions are dropped when a unit with master override reboots and then rejoins the HA cluster. This behavior is shown only when the primary unit is rebooted, or powered up, not when an interface is disconnected and reconnected.
- For a NAT outgoing policy with AV and IPS enabled in the protection profile, clients still can log in to MSN Messenger and initiate a chat session through the FortiGate firewall.
- When the "All" check box is used to control the URL block list, the change does not take effect until after a system reboot. The CLI exhibits the same behavior. You can use individual entry enable/disable to effect changes in the URL list to work around this.
- FortiGuard allows a denied site to be passed to the client when the page is reloaded again and again.

- When an IPSec dial-up client is using an address group for the source address, the FortiGate VPN Gateway firewall policy applies only to the last entry in the dial-up client address group. For example, on the FortiGate dial-up server, the encrypt policy source-to-destination is 192.168.2.0->all. On dialup client, 192.168.4.0+192.168.22.0(address group)->192.168.2.0. Then, the resulting dial-up encrypt firewall policy is 192.168.2.20->192.168.22.0.  
You can work around this by creating a dedicated tunnel on the VPN Gateway just for this client, with a matching policy, or make the client initiate separate tunnels for each address subnet.
- A Dynamic DNS defined VPN gateway address can be configured the Phase1 settings. The IPSec tunnel will not start-up when triggered by appropriate firewall policy traffic. This does not affect the DynDNS interface functionality (DDNS enable). Determine the resolved FQDN for the remote VPN gateway from the CLI exec ping <vpn-gw-fqdn-addr>. Contact Customer Support for an interim solution.
- Dialup IPSec policies cannot match the correct Phase 2 configuration when multiple Phase 2 names share the same base name string and only differ by a numeric suffix, for example, p2 and p22 are not distinguished. The workaround is to use Phase 2 tunnel names that do not share the same base string or names that only differ by a suffix.
- After a reboot of the FortiGate firewall, all logging messages for Syslog and FortiLog servers are not sent, although the memory and local hard disk logging continue to operate normally. The woraround is to modify any Log Setting after a reboot to restart the Syslog and FortiLog processes.
- The DHCP relay agent for IPSec tunnels continues to use the old interface IP address after changing the IP address of the interface connected to the external DHCP server. Disable and then re-enable the DHCP relay function after changing the interface IP address.
- Due to browser caching behavior, the administrator cannot view any firewall policies in the summary policy webpage when clicking on the expand triangle icon. This behavior is most common to Mozilla and Netscape browsers, but may also occur with Microsoft Internet Explorer. Clear the browsers cache.
- Changing a local user's password does not take effect until after a reboot. This will affect changes to user authentication in firewall policies and dial-up IPSec tunnels using Peer ID group.

# New features and changes

In FortiOS 2.80, both the web-based manager and the CLI are redesigned for improved usability and convenience. There are also numerous new features and changes to existing features.

This chapter contains general information about the new features and changes based on upgrading from FortiOS 2.50MR10 to FortiOS 2.80MR11. See [“New features and changes for FortiOS 2.80MR8 to FortiOS 2.80MR10” on page 50](#) for specific changes and new features for other FortiOS 2.80 maintenance releases and [“New features and changes for FortiOS 2.80MR11” on page 65](#) for FortiOS 2.80MR11.

Before proceeding to upgrade your FortiGate unit, it is recommended to review this document and the following documents to familiarize yourself with the new features and changes.

- The [FortiGate Administration Guide](#) specific to your FortiGate unit.
- The [FortiGate CLI Reference Guide](#).
- The release notes of the firmware image.

The following topics are included in this section:

- [CLI command changes](#)
- [System](#)
- [Router](#)
- [Firewall](#)
- [User](#)
- [VPN](#)
- [IPS](#)
- [Antivirus](#)
- [Web Filter](#)
- [Spam Filter](#)
- [Log & Report](#)
- [HA](#)
- [Using Perl regular expression in FortiOS 2.80](#)
- [New features and changes for FortiOS 2.80MR8 to FortiOS 2.80MR10](#)
- [New features and changes for FortiOS 2.80MR11](#)



**Note:** Configuration of settings in the following menus are unchanged unless otherwise stated.



**Note:** Before upgrading to FortiOS 2.80, make sure you have the following documents:

- Administration and Installation Guides specific to your FortiGate unit
- *FortiGate 2.80 Maximum Values Matrix MR10*
- *VPN Guide* or *VPN QuickStart Guide*
- *Intrusion Protection System (IPS) Guide*

These guides provide additional information after upgrading to FortiOS 2.80.

## CLI command changes

The CLI commands in FortiOS 2.80, have significantly changed. The method of entering these commands, including their structure, navigation, command types, and command branches have changed as well.

The entire CLI command structure is viewed by typing the CLI command, `tree`. The following table outlines the changes in the top shell commands.

**Table 3: CLI command changes from 2.50 to 2.80**

| 2.50     | 2.80           | Description of changes                                                                                                                                                                                                           |
|----------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| set      | config,<br>set | The <code>config</code> command branch replaces the <code>set</code> command branch. This branch, <code>config</code> , uses configuration shells. The <code>set</code> command is still used for setting functional parameters. |
| unset    | unset          | The <code>unset</code> function has been moved under the <code>config</code> branch.                                                                                                                                             |
| get      | get            | The <code>get</code> command branch has some changes to how it functions                                                                                                                                                         |
| execute  | execute        | The <code>execute</code> command branch has been updated.                                                                                                                                                                        |
|          | show           | The <code>show</code> command branch is new.                                                                                                                                                                                     |
| diagnose | diagnose       | The <code>diagnose</code> command branch has been updated.                                                                                                                                                                       |

During the installation process, the existing FortiOS 2.50 configuration automatically upgrades to the FortiOS 2.80 configuration. These changes to the CLI are consistent throughout all FortiOS 2.80 maintenance releases.



**Note:** Review the CLI commands and CLI command structure from the CLI interface after upgrading to familiarize yourself with the changes and new features.

## System

The System menu consists of the following:

- [Status](#)
- [Network](#)
- [DHCP](#)
- [Config](#)
- [Admin](#)

- [Maintenance](#)
- [Virtual Domain](#)

## Status

The Status page displays the System Dashboard. The System Dashboard is a categorized summary of the FortiGate unit's activity and information.

The System Dashboard categories are:

- Alert Message Console
- Unit Information
- Recent Virus Detections
- Content Summary
- Interface status
- System Resources
- Recent Intrusion Detections

The Status menu includes the Sessions tab. However, the Monitor tab is now located in **System > Status > System Resources** category. Also, the up time for the FortiGate unit is now located at the bottom of the screen in the web-based manager.

## Sessions

The Sessions tab now provides filtering for sessions. You can also display the virtual domain root or all virtual domains from this tab.

## Network

The Network menu enables you to configure interfaces and zones to group related interfaces, including VLAN interfaces. You can also configure DNS settings along with more advanced network settings. The Network menu consists of the following tabs: Interface, Zone, DNS, and Modem.

The Zone tab enables you to group related interfaces and VLAN subinterfaces. This provides simpler policy creation. Also, you can configure policies for connections to and from a zone, rather than each interface and subinterface.

The Modem tab, available on FortiGate units with modem capabilities, enables you to configure your FortiGate modem for Standalone mode or Redundant mode. See your *FortiGate Administration Guide* for your specific FortiGate unit for more information.



**Note:** The Routing Table is only available in Transparent mode. Also, the DHCP tab in FortiOS 2.50 is now a menu in the System menu.

## DHCP

From the DHCP menu, you can configure a DHCP server or a DHCP relay agent on any FortiGate interface or any VLAN subinterface. The FortiGate interface can act as either a DHCP server or a DHCP relay agent, but not both at the same time.

The DHCP menu has the following tabs:

- [Service](#)
- [Server](#)
- [Exclude Range](#)
- [IP/Mac Binding](#)
- [Dynamic IP](#)



**Note:** Your FortiGate unit must be in NAT/Route mode to configure a DHCP server or DHCP relay agent. A static IP address is needed to configure a DHCP server or DHCP relay agent to that interface.

### Service

The Service tab enables you to configure DHCP services on each interface. You can turn off DHCP services from this tab as well.

### Server

The Server tab enables you to add more than one DHCP server to a single interface to provide DHCP services to multiple networks. The interface assigns an IP address to hosts on a network connected to the interface, as a DHCP server.

### Exclude Range

The Exclude Range tab enables you to add up to sixteen exclude ranges of IP addresses that FortiGate DHCP servers cannot assign to DHCP clients. These exclude ranges apply to all FortiGate DHCP servers.

### IP/Mac Binding

The IP/Mac Binding tab enables you to reserve an IP address for a particular device on the network according to the MAC address of the device. When you add the MAC address and an IP address to the IP/Mac Binding list, the DHCP server always assigns this IP address to the MAC address. IP/Mac Binding pairs apply to all FortiGate DHCP servers.

### Dynamic IP

The Dynamic IP tab enables you to view the list of IP addresses the DHCP server has assigned, including their corresponding MAC addresses. This tab displays the expiry time and date for these IP addresses.

## Config

The Config menu now has two new tabs, HA for high availability, and FortiManager for configuring a connection to a FortiManager unit. There are several new options for all tabs in the Config menu. For example, on higher-end FortiGate units, you can configure a pin protection password for an LCD panel.

The HA tab is available on most FortiGate units, and enables you to configure high availability for your FortiGate unit. FortiGate HA consists of two or more FortiGate units operating as a HA cluster. The network sees the HA cluster as a single FortiGate unit that processes network traffic and provides normal security services.

See the *FortiGate High Availability Guide* for more information or the *FortiGate Administration Guide's* HA section in the System Config chapter for your specific FortiGate unit.

The SNMP v1/v2c tab now provides you with configuring up to three SNMP communities in FortiOS 2.80. An SNMP community is a grouping of equipment for network administration purposes. When you add SNMP communities, it allows SNMP managers to connect to the FortiGate unit to view system information and receive SNMP traps. The FortiGate unit allows up to three SNMP communities. A community can have a different configuration for SNMP queries and traps. The community can be configured to monitor the FortiGate unit for a different set of events. You can add IP addresses of up to eight SNMP managers to each community.

The Replacement Messages tab now includes multiple options to customize your alert emails. When you select the blue arrow, you expand the options for each replacement message.

The FortiManager tab enables you to configure the FortiGate unit to connect with a FortiManager unit. When you enable this feature, all communication between the FortiGate unit and the FortiManager Server takes place using VPN.



**Note:** The Admin tab is now a menu in System menu. Also, the HA tab may not be available on lower-end units. For example, the FortiGate-50A does not have a HA tab.



**Note:** Replacement messages need to be manually updated in FortiOS 2.80. See [“Backing up your replacement messages” on page 76](#) and [“Converting your replacement messages to FortiOS 2.80” on page 79](#) for more information.

## Admin

The Admin menu is new for FortiOS 2.80. Similar to the Admin tab in **System > Config** in FortiOS 2.50, the Admin menu enables you to configure, edit, and add administrators. From the Admin menu you can control the access level of each administrator account including control over the IP address where the administrator connects to the FortiGate unit.

Each account refers to an Access profile, located in the Access Profile tab in the Admin menu. An admin administrator with read and write access profiles can create profiles for other administrators. These administrators can have only read access privileges over certain access controls, or read and write privileges and access to all access controls. These access controls are:

- System Configuration
- Log and Report
- Security Policy
- Auth Users
- Admin Users
- FortiProtect Update
- System Shutdown

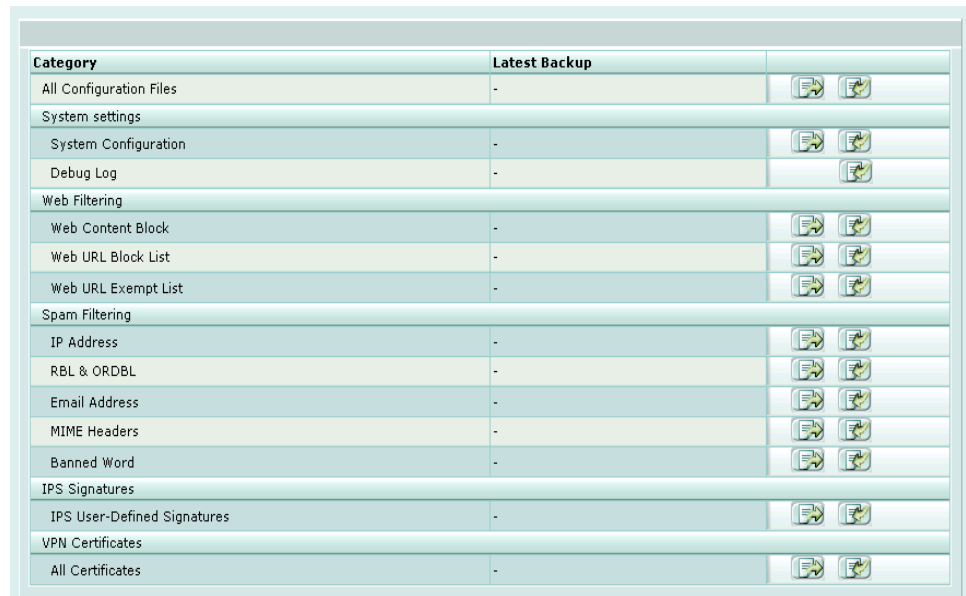
In FortiOS 3.0, the FortiGate unit is limited to 8, 16 or 64 administrator accounts depending on the unit. For example, the FortiGate-50A can only hold 8 while the FortiGate-200 can hold 16. The FortiGate-1000 and above can hold 64 administrator accounts. See *FortiGate FortiOS 2.80 Maximum Values Matrix MR10 and up* for more information concerning the maximum value of administrator accounts and other similar information.

## Maintenance

The Maintenance menu enables you to back up and restore configuration files, or update antivirus and attack definitions. You can also shutdown your FortiGate unit, reboot the FortiGate firewall, or reset your configuration settings to factory default settings from the Maintenance tab.

The Backup and Restore tab enables you to either backup your existing FortiOS 2.80 configuration or restore your FortiOS 2.80 configuration. You can backup individual files such as MIME Headers and Web URL Block list.

**Figure 6: Backup and Restore page**



| Category                    | Latest Backup |                    |
|-----------------------------|---------------|--------------------|
| All Configuration Files     | -             | [Backup] [Restore] |
| System settings             |               |                    |
| System Configuration        | -             | [Backup] [Restore] |
| Debug Log                   | -             | [Backup]           |
| Web Filtering               |               |                    |
| Web Content Block           | -             | [Backup] [Restore] |
| Web URL Block List          | -             | [Backup] [Restore] |
| Web URL Exempt List         | -             | [Backup] [Restore] |
| Spam Filtering              |               |                    |
| IP Address                  | -             | [Backup] [Restore] |
| RBL & ORDBL                 | -             | [Backup] [Restore] |
| Email Address               | -             | [Backup] [Restore] |
| MIME Headers                | -             | [Backup] [Restore] |
| Banned Word                 | -             | [Backup] [Restore] |
| IPS Signatures              |               |                    |
| IPS User-Defined Signatures | -             | [Backup] [Restore] |
| VPN Certificates            |               |                    |
| All Certificates            | -             | [Backup] [Restore] |

The Update Center tab enables you to configure the FortiGate unit to connect to the FortiProtect Distribution Network (FDN) to update the antivirus and attack definitions. You can configure the FortiGate unit to allow push updates on the Update Center page. Push updates are provided from the FDN using HTTPS on UDP port 9443. The FDN must be able to route packets to the FortiGate unit using UDP port 9443 to receive updates.

Figure 7: Update Center page

FortiProtect Distribution Network: ●

Push Update: ● Refresh

Use override server address

| Update                                   | Version | Expiry date | Last update attempt | Last Update Status |
|------------------------------------------|---------|-------------|---------------------|--------------------|
| FortiGuard - AV Engine                   | 1.077   | n/a         | n/a                 | Installed updates  |
| FortiGuard - AV Definition               | 6.123   | n/a         | n/a                 | Installed updates  |
| FortiGuard - Intrusion Definition        | 2.240   | n/a         | n/a                 | Installed updates  |
| FortiGuard - Intrusion Protection Engine | 1.000   | n/a         | n/a                 | Installed updates  |

**Allow Push Update**

Use override push IP  Port

**Scheduled Update**

Every:  (hour)

Daily:  (hour)

Weekly:  (day)  (hour)

Apply Update Now

The Support tab enables you to report problems with your FortiGate unit to Fortinet Technical Support or to register your FortiGate unit with the FortiProtect Distribution Server (FDS). The option, Report Bug, enables you to submit problems to Fortinet Technical support. The other option, FDS Registration, enables you to register your FortiGate unit with Fortinet.

The Shutdown tab enables you to log out, reboot the FortiGate firewall, reset to factory default settings, or shutdown the FortiGate unit. When you select Reset to Factory Default settings, all configuration settings are lost and interface addresses revert to factory default settings.



**Note:** You can also log out by selecting the Log out icon, located at the top right corner of the web-based manager.

## Virtual Domain

The Virtual Domain menu is new for FortiOS 2.80. FortiGate virtual domains provide multiple logical firewalls and routers in a single FortiGate unit. For example, one FortiGate unit can provide exclusive firewall and routing services to multiple networks so traffic from each network is effectively separated from other networks.

With a virtual domain, you can develop and manage:

- interfaces
- VLAN subinterfaces
- zones
- firewall policies
- routing
- VPN configuration for each virtual domain (separately)

Virtual Domains are similar in both NAT/Route mode and Transparent mode since the interfaces, VLAN subinterfaces, zones, firewall policies, routing and VPN configurations are shared. The major difference is that in Transparent mode, interfaces and VLAN interfaces do not have IP addresses and routing is simplified.



**Note:** The FortiGate unit supports only two virtual domains, a root domain and one additional domain. You cannot delete the root virtual domain. Also, if you require more information, see the *FortiGate VLAN and VDOM Guide* or your *FortiGate Administration Guide's* chapter System Network, VLAN section.

## Router

The Router menu, new to FortiOS 2.80, consists of the following menus:

- [Static](#)
- [Policy](#)
- [RIP](#)
- [Router Objects](#)
- [Monitor](#)

### Static

The Static menu has one tab, the Static tab. A static route specifies where to forward packets that have a particular destination IP address. Static routes control traffic exiting the FortiGate unit. You can specify through which interface the packet will leave and which device the packet should be routed.

You can configure routes by defining the destination IP address and netmask of packets the FortiGate unit is configured to intercept. You can also specify a gateway IP address for those packets. The gateway address specifies the next hop router where the traffic will be routed.



**Note:** The value 0.0.0.0/0.0.0.0 (all destinations) is reserved for the default route. You must specify a gateway address and outbound interface for the default route to route packets according to the default route.

### Policy

The Policy menu consists of one tab, Policy Route. With policy routing you can configure the FortiGate unit to route packets based on:

- source address
- protocol
- service type
- port range
- incoming or source interface

The FortiGate unit begins at the top of the policy routing list, then attempts to match the packet with a policy. The policy route supplies the next hop gateway including the FortiGate interface to use by the traffic. The FortiGate unit routes the packet using the regular routing table if no policy route matches the packet,.

## RIP

The Routing Information Protocol (RIP) menu consists of the following tabs:

- [General](#)
- [Networks](#)
- [Interface](#)
- [Distribution List](#)
- [Offset List](#)

The FortiGate implementation of RIP supports both RIP version 1 as defined by RFC 1058, and RIP version 2 as defined by RFC 2453. RIP version 2 enables RIP messages to carry more information, and to support simple authentication and subnet masks. RIP is a distance-vector routing protocol intended for small, relatively similar networks. RIP uses hop count as its routing metric. Each network is usually counted as one hop. The network diameter is limited to 15 hops.

### General

The General tab enables you to configure general RIP settings, such as RIP version.

### Networks

The Networks tab enables you to identify the networks of where to send and receive RIP updates. If a network is not specified, interfaces in that network will not be advertised in RIP updates.

### Interface

The Interface List tab enables you to configure RIP Version 2 authentication, including RIP version send and receive for a specified interface. You can also configure and enable split horizon. Authentication is only available for RIP Version 2 packets that send and receive by an interface. You should set authentication to None, if the Send Version or Recent Version options are set to one or twelve.

### Distribution List

The Distribution List enables you to filter incoming or outgoing updates, using an access list or a prefix list. The filter will be applied to all interfaces in the current virtual domain if you do not specify an interface.



**Note:** By default, all distribution lists for the root domain are displayed. If you create an additional virtual domain, only the distribution lists belonging to the current virtual domain are displayed. Go to **System > Virtual Domain > Virtual Domains** to view the settings associated with a different virtual domain and select the virtual domain.

### Offset List

The Offset List enables you to add specific offsets to the metric of a route.

## Router Objects

The Router Objects menu consists of the following tabs:

- [Access List](#)
- [Prefix List](#)
- [Route-map](#)

This menu enables you to configure router objects, a set of tools used by routing protocols and features.

### Access List

The Access List tab enables you to configure access lists. These lists are filters used by the FortiGate routing features. Each rule in an access list consists of the following:

- a prefix, which is an IP address and a netmask
- the action to take for this prefix (permit or deny)
- whether to match the prefix exactly or match the prefix with a specific prefix

An access list must be called by another FortiGate routing feature, such as RIP or OSPF, before it can take effect.

### Prefix List

The Prefix List tab is an enhanced version of an access list. A prefix list enables you to control the length of the prefix netmask. The prefix list must be called by another FortiGate routing feature, such as RIP or OSPF, before it can take effect.

### Route-map

The Route-map tab enables you to configure route-maps. These maps are a specialized form of filtering. Route-maps are similar to access lists, but have enhanced matching criteria. These maps can be configured to make changes as defined by a set of statements, including permit and deny actions.

The FortiGate unit attempts to match the rules in a route-map starting at the top of the list. If it finds a match, it makes the changes defined in the set statements and then takes the action specified for the rule. If no match is found in the route-map, the default action is deny. If no match statements are defined in a rule, the default action is to match everything. If multiple match statements are defined in a rule, all the match statements must match before the set statements can be used.



**Note:** A route-map can only take effect if its called by another FortiGate routing feature, such as RIP.

### Key-chain

The Key-chain tab enables you to configure key-chain lists. A key-chain is a list of one or more keys including the send and receive lifetimes for each key. The RIP Version 2 protocol is used to authenticate keys to ensure routing information exchange between routers is reliable. Both the sending and receiving routers must be set to use authentication, including configured with the same keys for authentication to work.

These keys are used for authenticating routing packets only, during the specified key lifetimes. The FortiGate unit migrates from one key to the next, according to the scheduled send and receive lifetimes.



**Note:** The sending and receiving routers should synchronize their dates and times for key lifetimes to prevent overlapping. However, overlapping the key lifetimes ensures a key is always available, even if there is a difference in the system times.

## Monitor

The Monitor menu has one tab, the Routing Monitor tab. This tab displays the entries in the FortiGate routing table. You can apply a filter to display certain routes and/or to search for specific routing protocols.

## Firewall

The IP/Mac Binding for the Firewall menu in FortiOS 2.50 is now located as a tab in **System > DHCP**. Content Profile is now Protection Profile in FortiOS 2.80. See your *FortiGate Administration Guide* for your specific FortiGate unit for more information.

## User

In the Local menu, the option Try other servers if connect to selected server fails, is no longer available.

## VPN

VPNs are configured slightly differently in FortiOS 2.80. It is recommended to review the *FortiGate VPN Guide* and/or the *FortiGate VPN Quick Start Guide* before proceeding to configure VPNs in FortiOS 2.80.

## IPSec

The IPSec menu's tabs are re-arranged in FortiOS 2.80. They appear in the following order:

- Phase 1
- Phase 2
- Manual Key
- Concentrator
- Ping Generator
- Monitor

The Ping Generator tab is new for FortiOS 2.80 and the Display Monitor tab in FortiOS 2.50 is renamed Monitor for FortiOS 2.80.

The Ping Generator tab enables you to configure a ping generator when no traffic in an IPsec VPN tunnel is being generated inside the tunnel. For example, a ping generator is useful in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically – traffic may be suspended while the IP address changes. You can also use a ping generator to troubleshoot network connectivity inside a VPN tunnel.

You can configure settings to generate ping commands through two tunnels simultaneously. The ping interval is fixed at 40 seconds. The source and destination IP addresses refer to the source and destination addresses of IP packets that will be transported through the VPN tunnel. When source and destination addresses of 0.0.0.0 are entered, no ping traffic is generated between the source and destination.

## PPTP

In the PPTP menu, you can now either enable or disable PPTP whether you have configured IPsec VPN or not. The L2TP menu is the same.



**Note:** The Certificate menu is unchanged. See your *FortiGate Administration Guide* for your specific FortiGate unit, for more information on configuring certificates in FortiOS 2.80.

## IPS

The IPS menu, new for FortiOS 2.80, consists of the following menus:

- [Signature](#)
- [Anomaly](#)

The IPS menu enables you to configure Intrusion Protection System custom signatures and anomalies. With IPS enabled, the FortiGate unit can record:

- suspicious traffic in logs
- send alert email to system administrators
- log, pass, drop, reset or clear suspicious packets or sessions

You can adjust some IPS anomaly thresholds to work best with normal traffic on protected networks. You can also create custom signatures to customize the FortiGate IPS for diverse network environments.

You can configure IPS globally and then enable or disable all signatures or all anomalies in individual firewall protection profiles.

If you require more information about IPS, see your *FortiGate Administration Guide* for your specific FortiGate unit or the *FortiGate Intrusion Protection System (IPS) Guide*.

### Signature

The Signature menu has two tabs, Predefined and Custom. The Predefined tab enables you to modify each signature, if required. The Custom tab enables you to create new custom signatures. You can enable logging for each custom signature from the Custom tab.

## Anomaly

The Protocol Anomaly is a new menu. The Protocol Anomaly detects and identifies network traffic that attempts to take advantage of known exploits.

## Antivirus

The Antivirus menu is now located below the IPS menu. This menu provides configuration access to most antivirus options when you create and enable a firewall protection profile. You can also implement specific settings on a per profile basis, even though antivirus settings are configured for system-wide use.

There is an order to antivirus operations. Antivirus processing includes various modules and engines that perform separate tasks. The order the features appear in the web-based manager is how the FortiGate unit performs antivirus processing. For example, the web-based manager menu may have an antivirus order similar to the following:

- file block
- virus scan
- grayware
- heuristics (configured only in the CLI)

By using the FDN, FortiProtect services provide an excellent resource of virus list updates and information. FortiProtect services also include automatic updates of virus and IPS (attack) engines and definitions, as well as local spam DNSBL.

## File Block

The File Block menu is slightly different in FortiOS 2.80 than in FortiOS 2.50. You can still configure file blocking to remove all files that are a potential threat and to prevent active computer virus attacks. However, file block entries are not case sensitive. For example, adding.exe to the file block list also blocks any files with an.EXE ending.

You can choose to disable file blocking in the Protection Profile, and enable it only to temporarily block specific threats as they occur. You can also enable or disable file blocking by protocol for each file pattern you configure. If both file block and virus scan are enabled, the FortiGate unit blocks files that match enabled file patterns and does not scan these files for viruses.

FortiGate units with a local disk can quarantine blocked and infected files. These files are displayed in the Quarantine files list. You can sort through the files by file name, date, service, status, duplicate count (DC), or time to live (TTL). You can filter the list as well to view only quarantined files with a specific status or from a specific service.

The AutoSubmit list enables you to configure the FortiGate unit to upload suspicious files to Fortinet for analysis. Enable automatic uploading of the configured file by going to **Anti-Virus > Quarantine > Config**.

## Config

The Config menu has a new tab, Grayware. The Grayware tab displays grayware programs. Grayware programs are unsolicited commercial software programs that are installed on computers, often without the user's consent or knowledge. Grayware programs can cause system performance problems or be used for malicious means.

The FortiGate unit scans for known grayware executable programs in each enabled category. The category list and contents are added or updated whenever your FortiGate unit receives a virus update package. New categories may be added at any time and will be loaded with the virus updates. By default all new categories are disabled. Grayware is enabled in a protection profile when Virus Scan is enabled.

Grayware categories are populated with known executable files. Each time the FortiGate unit receives a virus and attack definitions update, the grayware categories and contents are updates.



**Note:** For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes less than the configured oversize threshold.

## Web Filter

The Web Filter menu has a new tab, Category Block. In FortiOS 2.80, the FortiGate unit performs web filtering in the order the files appear in the web-based manager. The files appear in the following order:

- content block
- URL block
- URL exempt
- category block (FortiGuard)
- script filter



**Note:** FortiGate web pattern blocking supports standard regular expression. You can add up to 20 patterns to the web pattern block list.

### URL Block

The URL Block menu is similar to FortiOS 2.50. However, you activate URL block settings by enabling **Web Filtering > Web URL Block** in your firewall Protection Profile. URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to ftp://ftp badsite.com. Use firewall policies to deny FTP connections instead.

The Web Pattern Block tab enables you to use regular expressions to define URL patterns.

## Category Block

In the Category Block menu, you can enable FortiGuard web filtering configuration from the Configuration tab. You can also have a URL's category re-evaluated from the Configuration tab.

The Category Block menu enables you to use Perl regular expressions or wildcards to add banned word patterns to the list. Perl is a programming language specially designed for processing text. Perl regular expression patterns are case sensitive for web filter content block. You can make a word or phrase case sensitive by using the regular expression `/i`. For example, `/bad language/i` blocks all instances of bad language regardless of case. However, wildcard patterns are not case sensitive.

In the Category Block menu, you can also add one or more banned words or patterns to block web pages containing these words. Banned words can be one word or a text string of up to 80 characters long. The maximum number of banned words in lists is 32.

The Category Block menu can generate reports on FortiGate units with a local disk. You can generate a text and pie chart format report on web filtering for any profile. The FortiGate unit maintains statistics for allowed, blocked and monitored web pages for each category. You can view reports for a range of hours or days, or you can view a complete report of all activity.

## Script Filter

The Script filter is unchanged in FortiOS 2.80. You need to activate script filtering settings by enabling **Web Filtering > Web Script Filtering** in your firewall Protection Profile. Some web pages may not function and display correctly when blocking Java Applet, Cookie and Active X.

## Spam Filter

The Spam Filter menu, new to FortiOS 2.80, consists of the following menus:

- [FortiGuard-AntiSpam](#)
- [IP Address](#)
- [DNSBL and ORDBL](#)
- [Email Address](#)
- [MIME Headers](#)
- [Banned Word](#)

The Spam Filter menu provides you with enabling FortiGuard Anti-Spam service and configuration on the FortiGuard-AntiSpam tab.

The Spam Filter menu provides configuration access to the spam filtering options you enable when you create a firewall protection profile. While spam filters are configured for system-wide use, you can enable the filters on a per profile basis. Spam filters can be configured to manage unsolicited commercial email by detecting spam email messages and identifying transmissions from known or suspected spam servers.

The order of spam filter operations may vary between SMTP and IMAP or POP3 traffic because some filters only apply to SMTP traffic (IP address and HELO DNS lookup). Filters that require a query to a server and a reply (FortiGuard and DNSBL/ORDBL) are run simultaneously. Queries are sent while other filters are running to avoid delays. The first reply to trigger a spam action will take effect as soon as the reply is received.

Incoming email is passed through the spam filters in the order the filters appear in the spam filtering options list, in a firewall protection profile. For example, the spam filter options list may appear similar to the following:

- FortiGuard
- IP address
- DNSBL & ORDBL
- HELO DNS lookup
- email address
- return email DNS check
- MIME header
- banned word (content block)

## FortiGuard-AntiSpam

The FortiGuard Anti-Spam menu enables you to configure FortiGuard AntiSpam service and configuration. The FortiGuard AntiSpam filtering is an antispam service from Fortinet that includes an IP address black list, a URL black list, and spam filtering tools. For example, the IP address black list contains addresses of email servers known to generate Spam.

You can also enable caching for the FortiGuard IP address and URL block lists. When you enable caching, the FortiGate unit does not need to access the server each time the same IP address or URL appears as the source of the email, improving performance. The cache is configured to use six percent of the FortiGate RAM. When the cache is full, the least recently used IP address or URL is deleted.

## IP Address

The IP Address menu consists of the IP address tab where you can configure the FortiGate unit to filter email from specific IP addresses. See your *FortiGate Administration Guide* for your specific FortiGate unit for more information.

## DNSBL and ORDBL

The DNSBL and ORDBL menu enables you to configure the FortiGate unit to filter email by accessing DNSBL or ORDBL servers. DNSBLs are DNS-based Blackhole Lists and ORDBLs are Open Relay Database Lists. These lists are an effective way to tag or reject spam as it enters your system. These lists also act as domain name servers that match the domain of incoming email to a list of IP addresses known to send spam or allow spam to pass through. DNSBLs keep track of reported spam source addresses, and ORDBLs keep track of unsecured third party SMTP servers, known as open relays. Some spammers use these third party SMTP servers to send unsolicited bulk email.

The FortiGate uses UDP through port 53 to communicate with DNSBL servers. The FortiGate unit compares the IP address or domain name of the sender to any database lists configured. The unit then checks all servers in the list simultaneously. If a match is found, the corresponding protection profile action is taken and if no match is found, the email is passed on to the next spam filter.



**Note:** The FortiGate unit must be able to look up the server domain name on the DNS server to connect to the DNSBL or ORDBL server.

## Email Address

The Email Address menu enables you to filter incoming email by using email address lists. The FortiGate unit compares the email address or domain of the send to the lists in sequence. If a match is found, the corresponding protection profile action is taken. If no match is found, the email is passed on to the next spam filter.

## MIME Headers

The Multipurpose Internet Mail Extensions (MIME) headers menu enables you to configure MIME header lists and MIME header options. The MIME headers are added to email messages to describe content type and content encoding. For example, the type of text in the body of an email or the program that generated the email. The following are examples of MIME headers:

- X-mailer; outgluck
- X-Distribution: bulk
- Content\_Type: text/html
- Content\_Type: image/jpg

A MIME headers list can be used to mark email from certain bulk email programs or with certain types of content common in spam messages. In the MIME headers menu, you can choose to either mark the email as spam or clear for each header you configure.

The FortiGate unit compares the MIME header key-value pair of incoming email to the list pair in sequence. If a match is found, the corresponding protection profile action is taken. If no match is found, the email is passed on to the next spam filter.

You can use Perl regular expressions or wildcards to add MIME header patterns to the list. However, MIME header entries are case sensitive.

## Banned Word

The Banned Word menu enables you to control spam by blocking email containing specific words or patterns. You can configure a banned word list and select banned word options in the Banned Word tab.

In the Banned Word tab, you can enter one or more banned words to sort email containing those words in the email subject, body, or both. These words can be marked either as Spam or Clear and can be one word or a phrase up to 127 characters long.

If you enter a single word, the FortiGate unit blocks all emails that contain that word and if you enter a phrase, the unit blocks all emails containing that exact phrase.

The FortiGate unit searches for banned words in email messages. If a match is found, the corresponding protection profile action is taken. If no match is found, the email is passed to the recipient.

You can use Perl regular expressions or wildcards to add banned word patterns to the list. Perl regular expression patterns are case sensitive for Spam Filter banned words. You can use wildcard patterns because they are not case sensitive. You can make a word or phrase insensitive by using the regular expression `/i`. For example `/bad /language/i` will block all instances of bad language regardless of case.

## Log & Report

The Log and Report menu consists of the following menus:

- [Log Config](#)
- [Log Access](#)

For descriptions of log formats and specific log messages, see the *FortiGate Log Message Reference*.



**Note:** When you enable and configure the Log to Remote Host settings on the Log Setting page in FortiOS 2.50, those settings are carried forward to the Syslog server on the Log Setting page in FortiOS 2.80.

### Log Config

The Log Config menu is similar to the Log Setting menu in FortiOS 2.50. The Log Config menu consists of the following tabs:

- Log Settings
- Alert Email
- Log Filter

The Log Config menu has a new tab, Alert Email. You can configure an alert email for alerting you or someone else about logs. The Traffic Filter tab is renamed Log Filter.

### Log Settings

From the Log Settings tab, you can configure and enable the storing of log messages to a FortiLog unit, system memory, or a Syslog server. You can also configure and enable the storing of log messages to a remote computer running a NetIQ WebTrends firewall reporting server.

**Figure 8: Log Settings for configuring where your logged files are stored**

**Log Settings**

- Fortilog**
  - IP: 0.0.0.0
  - Level: Alert
  - Enable encryption
  - Local ID: [ ]
  - Pre-shared key: [ ]
- Memory**
  - Level: Alert
- Syslog**
  - Name/IP: [ ] Port: 514
  - Level: Alert
  - Facility: local7
  - Enable CSV Format
- WebTrends**
  - Name/IP: [ ]
  - Level: Alert

**Apply**

- FortiLog** A FortiLog unit. The FortiLog unit is a log analyzer and manager that can combine the log information from various FortiGate units and other firewall units. To enable content archiving with a firewall Protection Profile, you need to select the FortiLog option and define its IP address.
- Memory** The FortiGate system memory. The FortiGate system memory has a limited capacity and only displays the most recent log entries. Traffic and content logs cannot be stored in the memory buffer. When the memory buffer is full, the FortiGate unit begins to overwrite the oldest messages. All log entries are deleted when the FortiGate unit restarts.
- Syslog** A remote computer running a syslog server.
- Web Trends** A remote computer running a NetIQ WebTrends firewall reporting server. FortiGate log formats comply with WebTrends Enhanced Log Format (NELF) and are compatible with NetIQ WebTrends Security Reporting Center 2.0 and Firewall Suite 4.1.



**Note:** The logging severity level must be set to Notification when configuring the logging location for recording traffic log messages. Traffic log messages do not generally have a severity level higher than Notification. Also, you must enable traffic logging for specific interfaces and firewall policies so they can be logged.



**Note:** Make sure you contact a FortiLog administrator before configuring a connection between your FortiGate unit and a FortiLog unit. You need to have the correct IP address to ensure a successful connection.

## Log Filter

In the Log Filter tab, you can create a customized log filter based on the log types for each logging location you enable.

The following describes each log filter.

|                        |                                                                                                                                                                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Traffic Log</b>     | The Traffic Log records all traffic to and through the FortiGate interfaces. You can configure logging for traffic controlled by firewall policies and for traffic between any source and destination addresses. You can also apply global settings, such as session or packet log. |
| <b>Event Log</b>       | The Event Log records management and activity events, such as when a configuration has changed or a routing gateway has been added.                                                                                                                                                 |
| <b>Antivirus Log</b>   | The Antivirus Log records virus incidents in Web, FTP, and email traffic.                                                                                                                                                                                                           |
| <b>Web Filter Log</b>  | The Web Filter Log records HTTP content blocks, URL blocks including URL exempt events.                                                                                                                                                                                             |
| <b>Attack Log</b>      | The Attack Log records attacks detected and prevented by the FortiGate unit.                                                                                                                                                                                                        |
| <b>Spam Filter Log</b> | The Spam Filter Log records blocking of address patterns and content in IMAP and POP3 traffic.                                                                                                                                                                                      |



**Note:** The logging severity level must be set to Notification when configuring the logging location for recording traffic log messages. Traffic log messages do not generally have a severity level higher than Notification. You need to enable traffic logging for specific interfaces and firewall policies so they can be logged.

## Log Access

The Log Access menu enables you to view log messages by event, attack, anti-virus, web filter, or spam filter. You can customize your log messages by selecting the Column Settings icon. The column settings apply to what you want included in the display when only the formatted (not raw) display is selected.

## HA

In FortiOS 2.80, you can configure your FortiGate unit for high availability in the web-based manager, and is located in **System > Config > HA**. The HA tab is available on all FortiGate units in FortiOS 2.80.

There are several new features with HA in FortiOS 2.80. One feature, load balancing, offers FortiGate units in a cluster the ability to share the load of processing network traffic including providing security services. The cluster appears to your network as a single device, adding increased performance without changing your network configuration. Another feature is called failover. A failover is the ability of a HA cluster to continue providing firewall services after a failure occurs.

FortiGate HA is incompatible with PPP protocols, such as DHCP or PPPoE. You cannot switch to operating in HA mode if one or more interfaces is dynamically configured using DHCP or PPPoE. Configuring a FortiGate interface to be a DHCP server or a DHCP relay agent is not affected by HA operation. In HA mode, both PPTP and L2TP are supported.

The default priorities of a HA heartbeat are set for two interfaces, but you must set a heartbeat priority for at least one cluster interface. You enable heartbeat communication by entering a priority for an interface. You can disable heartbeat communication by deleting the priority of the interface. You should change the heartbeat device priorities only to control the interface used for heartbeat traffic, or the interface where heartbeat traffic reverts if the interface with the highest heartbeat priority fails or is disconnected.

You do not need to assign IP addresses to heartbeat device interfaces for them to be able to process heartbeat packets. The cluster assigns virtual IP addresses to the heartbeat device interfaces. For example, the primary cluster unit's heartbeat device interface is assigned the IP address 10.10.10.1, and a second cluster unit is assigned 10.10.10.2 and so on.

You can monitor HA interfaces to verify the interface is functioning properly and is connected to its network. However, you can only monitor physical interfaces, not VLAN subinterfaces.

If you require more information on HA and configuring a HA cluster, see the *FortiGate High Availability (HA) Guide* for more information.



**Note:** HA does not provide session failover for PPPoE, DHCP, PPTP, and L2TP services. Also, all members of a HA cluster must be set to the same HA mode.

## Using Perl regular expression in FortiOS 2.80

In both the Spam Filter menu and the Web Filter menu, you can use Perl regular expressions and wildcards to configure MIME headers, banned words, and email address lists. Perl is a programming language specially designed for processing text. If you require more information on Perl, see <http://www.perldoc.com/perl5.8.0/pod/perlre.html> for more information.

In Perl regular expressions, `.` character refers to any single character. It is similar to the `?` character in a wildcard match pattern. For example, `fortinet.com` can match `fortinetacom`, `fortinetbcom`, and `fortinetccom`.

In Perl regular expressions, the pattern does not have an implicit word boundary. For example, the regular expression `test` not only matches the word `test` but also matches any word that contains `test` such as `atest`, `mytest`, `testimony`, and so on. The notation `/b` specifies the word boundary. If you want to match the exact word `test`, the Perl expression should be `\btest\b`.

See your *FortiGate Administration Guide* for your specific FortiGate unit for more information on Perl regular expressions and wildcards when configuring MIME headers, banned words and email address lists in FortiOS 2.80.

# New features and changes for FortiOS 2.80MR8 to FortiOS 2.80MR10

The following is about the new features and changes for FortiOS 2.80MR8 to FortiOS 2.80MR10, including some procedures for certain features. The following also includes corrections for errata in documentation.

## Alert Message Console

The Alert Message Console is now included in the Status page in **System > Status**. This feature is located at the top of the Status page. You can read alert messages about system restarts, firmware upgrades, and Antivirus or IPS fail-open conditions.

## Unit Information

The following subscription service names have changed:

- Antivirus Definitions – FortiGuard-AV Definitions
- Attack Definitions – FortiGuard-Intrusion Definitions

## Preventing the public FortiGate interface from responding to ping requests

The factory default configuration of your FortiGate unit allows the default public interface to respond to ping requests. For the most secure operation, you should change the default configuration of the external interface so that it does not respond to ping requests. By changing the configuration, it makes it more difficult for a potential hacker to detect your FortiGate unit from the Internet.

Depending on the FortiGate unit, the default public interface can be the external or WAN1 interface, and with some FortiGate units, the default external interface has a port number, such as Port 2. See the FortiGate QuickStart Guide or the FortiGate Installation Guide for your FortiGate unit if you are unsure about the default external interface.

The following procedure enables you to disable ping access for the external interface of a FortiGate unit, whether in Transparent or NAT/Route mode.

### To disable ping administrative access from the web-based manager

- 1 Log into the FortiGate web-based manager.
- 2 Go to **System > Network > Interface**.
- 3 Choose the external interface and select Edit.
- 4 Clear the Ping Administrative Access checkbox.
- 5 Select OK to save the changes

### To disable ping administrative access from the FortiGate CLI

- 1 Log into the CLI.
- 2 Enter the following commands to disable administrative access to the external interface:

```
config system interface
 edit external
 unset allowaccess
 end
```

## Access Profile for prof\_admin

Except for the prof\_admin profile, all admin profiles can be edited. If you attempt to edit the prof\_admin profile in the Access Profile menu, a message “reserved keyword” displays.

## Subordinate units block multicast and broadcast traffic in HA

By default, a FortiGate HA cluster load balances virus scanning sessions among all of the cluster units. All other traffic is processed by the primary unit. You can configure the cluster to load balance TCP traffic and virus scanning among all cluster units by using the CLI. All UDP, ICMP, multicast, and broadcast traffic continues to be processed by the primary unit.

If you want to load balance TCP and virus scanning among all cluster units, enter the following command.

```
config system ha
 set load-balance-all enable
end
```

## Subordinate units, logging and SNMP in HA

Both the primary and subordinate units send traps to SNMP managers. Subordinate units first send traps to the primary units using the HA heartbeat device link. The primary unit then forwards the trap to SNMP managers. HA traps indicate when a cluster unit has started and when interfaces have been connected to disconnected.

All cluster units send log messages to a remote syslog server, FortiLog unit, and WebTrends server. Subordinate units first send log messages to the primary unit using the HA heartbeat device link. The primary unit forwards the log messages to the remote syslog server, FortiLog unit, and WebTrends server.

## Updating MAC forwarding tables when a link failover occurs in HA

When a FortiGate HA cluster is operating and a monitored interface fails on the primary unit, the primary unit usually becomes a subordinate unit and another cluster unit becomes the primary unit. After a link failover, the new primary unit sends special ARP packets to refresh the MAC forwarding tables, or arp tables, of the switches connected to the cluster. This is normal link failover operation.

Some high-end switches may not be able to detect that the primary unit has become a subordinate unit and will keep sending packets to the former primary unit. This occurs if the high end switch if the high end switch does not detect the failure and does not clear its MAC forwarding table.

To make sure the switch detects the failover and clears its MAC forwarding tables, use the following command to cause the primary unit to shut down all its interfaces, except the heartbeat device interfaces, for one second when a link failover occurs. If the primary unit interfaces are shut down for one second, the switch should be able to detect this failure and clear its MAC forwarding tables. When the new primary unit is operating, the switch can detect the special arp packets and update its MAC forwarding table correctly.

## Command syntax

```
config system ha
 set link-failed-signal enable
end
```

## FortiManager configuration

All communication between the FortiGate unit and the FortiManager server takes place using VPN after the following is enabled in **System > Config > FortiManager**.

**Enable FortiManager** Enable secure IPsec VPN communication between the FortiGate unit and a FortiManager server.

**FortiManager ID** Enter the serial number of the FortiManager server.

**FortiManager IP** Enter the IP address of the FortiManager server.

## FortiGate SNMP traps and fields

The FortiGate agent can send traps to SNMP managers added to SNMP communities. You must load and compile the Fortinet trap MIB, file name `fortinet.trap.2.80.mib`, onto the SNMP manager for SNMP managers to receive traps.

All traps include the trap message as well as the FortiGate unit serial number.

**Table 4: Generic FortiGate traps**

| Trap message                                 | Description                              |
|----------------------------------------------|------------------------------------------|
| ColdStart<br>WarmStart<br>LinkUp<br>LinkDown | Standard traps as described in RFC 1215. |

**Table 5: FortiGate system traps**

| Trap message                            | Description                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU usage high<br>(fnTrapCpuHigh)       | CPU usage exceeds 90%.                                                                                                                                                                                                                                                                                                  |
| Memory low<br>(fnTrapMemLow)            | Memory usage exceeds 90%.                                                                                                                                                                                                                                                                                               |
| Interface IP change<br>(fnTrapIpChange) | Change of IP address on a FortiGate interface. The trap message includes the name of the interfaces, the new IP address of the interface, and the serial number of the FortiGate unit. This trap can be used to track interface IP changes for interfaces configured with dynamic IP addresses set using DHCP or PPPoE. |

**Table 6: FortiGate VPN traps**

| Trap message                             | Description                     |
|------------------------------------------|---------------------------------|
| VPN tunnel is up<br>(fnTrapVpnTunUp)     | An iPSec VPN tunnel started.    |
| VPN tunnel is down<br>(fnTrapVpnTunDown) | An IPsec VPN tunnel shuts down. |

**Table 7: FortiGate IPS traps**

| Trap message                          | Description             |
|---------------------------------------|-------------------------|
| IPS Anomaly<br>(fnTrapIpsAnomaly)     | IPS anomaly detected.   |
| IPS Signature<br>(fnTrapIpsSignature) | IPS signature detected. |

**Table 8: FortiGate antivirus traps**

| Trap message                      | Description                                                                                                             |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Virus detected<br>(fnTrapAvEvent) | The FortiGate unit detects a virus and removes the infected file from an HTTP or FTP download or from an email message. |

**Table 9: FortiGate IM traps**

| Trap message                                 | Description                                     |
|----------------------------------------------|-------------------------------------------------|
| White/black list full<br>(fnTrapImTableFull) | The FortiGate unit IM white/black list is full. |

**Table 10: FortiGate logging traps**

| Trap message                              | Description                                                                                                                                          |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Flag event count<br>(fnTrapFlgEventCount) | FortiLog Events number exceeds limit.                                                                                                                |
| Log full (fnTrapLogFull)                  | On a FortiGate unit with a hard drive, hard drive usage exceeds 90%. On a FortiGate unit without a hard drive, log to memory usage has exceeded 90%. |

**Table 11: FortiGate HA traps**

| Trap message                      | Description                                                                                                                            |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| HA state<br>(fnTrapHaStateChange) | HA state change. The trap message includes the previous state, the new state and flag indicating whether the unit is the primary unit. |
| HA switch<br>(fnTrapHaSwitch)     | The primary unit in a HA cluster fails and is replaced with a new primary unit.                                                        |

**Table 12: FortiBridge traps**

| Trap message                               | Description                                          |
|--------------------------------------------|------------------------------------------------------|
| FortiBridge detects fail<br>(fnTrapBridge) | A FortiBridge unit detects a FortiGate unit failure. |

## FortiGate MIB fields

The Fortinet MIB contains fields reporting current FortiGate unit status information. The tables below list the names of the MIB fields and describes the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the `fortinet.2.80.mib` file into your SNMP manager and browsing the Fortinet MIB fields.

**Table 13: System MIB fields**

| MIB field        | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| fnSysModel       | FortiGate model number, for example, 400, for the FortiGate-400.         |
| fnSysSerial      | FortiGate unit serial number.                                            |
| fnSysVersion     | The firmware version currently running on the FortiGate unit.            |
| fnSysVersionAv   | The antivirus definition version installed on the FortiGate unit.        |
| fnSysVersionNids | The attack definition version installed on the FortiGate unit.           |
| fnSysHaMode      | The current FortiGate High-Availability (HA) mode (standalone, A-A, A-P) |
| fnSysOpMode      | The current FortiGate unit operation mode (NAT or Transparent).          |
| fnSysCpuUsage    | The current CPU usage (as a percent).                                    |
| fnSysMemUsage    | The current memory utilization (in MIB).                                 |
| fnSysSesCount    | The current IP session count.                                            |

**Table 14: HA MIB fields**

| MIB field          | Description                                                                                                |
|--------------------|------------------------------------------------------------------------------------------------------------|
| fnHaGroupId        | HA Group ID.                                                                                               |
| fnHaPriority       | The clustering priority of the individual FortiGate unit in a cluster.                                     |
| fnHaOverride       | The primary-override setting (enable or disable) for an individual FortiGate unit in a cluster.            |
| fnHaAutoSync       | Auto config synchronization flag.                                                                          |
| fnHaSchedule       | Load balancing schedule for A-A mode                                                                       |
| fnHaStatsTable     | Statistics for all the individual FortiGate unit in the HA cluster.                                        |
| fnHaStatsIndex     | The index number of the unit in the cluster.                                                               |
| fnHaStatsSerial    | The FortiGate unit serial number.                                                                          |
| fnHaStatsCpuUsage  | The current FortiGate unit CPU usage (%).                                                                  |
| fnHaStatsMemUsage  | The current unit memory usage (MB).                                                                        |
| fnHaStatsNetUsage  | The current unit network utilization (Mbps).                                                               |
| fnHaStatsSesCount  | The number of active sessions being processed by the FortiGate unit.                                       |
| fnHaStatsPktCount  | The number of packets processed by the FortiGate unit.                                                     |
| fnHaStatsByteCount | The number of bytes processed by the FortiGate unit.                                                       |
| fnHaStatsIdsCount  | The number of attacks detected by the IPS running on the FortiGate unit in the last 20 hours.              |
| fnHaStatsAvCount   | The number of viruses detected by the antivirus system running on the FortiGate unit in the last 20 hours. |

**Table 15: Administrator accounts**

| MIB field     | Description                                         |                                                                                      |
|---------------|-----------------------------------------------------|--------------------------------------------------------------------------------------|
| fnAdminNumber | The number of administrators on the FortiGate unit. |                                                                                      |
| fnAdminTable  | Table of administrators                             |                                                                                      |
|               | fnAdminIndex                                        | Administrator account index number.                                                  |
|               | fnAdminName                                         | The user name of the administrator account.                                          |
|               | fnAdminAddr                                         | An address of a trusted host or subnet where this administrator account can be used. |
|               | fnAdminMask                                         | The netmask for fnAdminAddr.                                                         |

**Table 16: Local users**

| MIB field    | Description                                      |                                                                                                                                                                                                                                                                                                                      |
|--------------|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fnUserNumber | The number of local users on the FortiGate unit. |                                                                                                                                                                                                                                                                                                                      |
| fnUser Table | Table of local users.                            |                                                                                                                                                                                                                                                                                                                      |
|              | fnUser Index                                     | Local user account index number.                                                                                                                                                                                                                                                                                     |
|              | fnUserName                                       | The user name of the local user account.                                                                                                                                                                                                                                                                             |
|              | fnUserAuth                                       | The authentication type for the local user:<br><b>local</b> – a password stored on the FortiGate unit<br><b>radius-single</b> – a password stored on a RADIUS server<br><b>radius-multiple</b> – any user who can authenticate on the RADIUS server can log on<br><b>ldap</b> – a password stored on an LDAP server. |
|              | fnUserStats                                      | Whether the local user is enabled and disabled.                                                                                                                                                                                                                                                                      |

**Table 17: Options**

| MIB field        | Description                                                                        |
|------------------|------------------------------------------------------------------------------------|
| fnOptidleTimeout | The idle period in minutes, and after this the administrator must re-authenticate. |

**Table 18: Virtual Domains**

| MIB field  | Description                                          |                                                             |
|------------|------------------------------------------------------|-------------------------------------------------------------|
| fnVdNumber | The number of virtual domains on the FortiGate unit. |                                                             |
| fnVdTable  | Table of virtual domains.                            |                                                             |
|            | fnVdIndex                                            | Internal virtual domain index number of the FortiGate unit. |
|            | VdName                                               | The name of the virtual domain.                             |

**Table 19: Active IP Sessions**

| MIB field        | Description                                                 |
|------------------|-------------------------------------------------------------|
| fnIpSessIndex    | The index number of the active IP session.                  |
| fnIpSessProto    | The IP protocol (TCP, UDP, ICMP, etc.) of the session.      |
| fnIpSessFromAddr | The source IP address of the active IP address.             |
| fnIpSessFromPort | The source port of the active IP session.                   |
| fnIpSessToPort   | The destination IP address of the active IP session.        |
| fnIpSessToAddr   | The destination port of the active IP session.              |
| fnIpSessExpiry   | The expiry time or time-to-live in seconds for the session. |

**Table 20: Dialup VPNs**

| MIB field           | Description                                           |
|---------------------|-------------------------------------------------------|
| fnVpnDialupIndex    | The index of the dialup VPN peer.                     |
| fnVpnDialupGateway  | The remote gateway IP address.                        |
| fnVpnDialupLifetime | VPN tunnel lifetime in seconds.                       |
| fnVpnDialupTimeout  | Time remaining until the next key exchange (seconds). |
| fnVpnDialupSrcBegin | Remote subnet address.                                |
| fnVpnDialupSrcEnd   | Remote subnet mask.                                   |
| fnVpnDialupDstAddr  | Local subnet address.                                 |
| fnVpnDialupDstMask  | Local subnet mask.                                    |

**Table 21: IPS**

| MIB field     | Description                                         |
|---------------|-----------------------------------------------------|
| fnIpsSigId    | The IPS signature ID.                               |
| fnIpsSigSrcIp | The source IP address of the IPS signature trigger. |

## Chassis status – FortiGate-5000

The following is information about the chassis status of the FortiGate-5000 series units.

### SMC

You can check the status of your shelf manager cards in **System > Chassis > SMC** in the web-based manager. On the SMC page, the following displays:

|                         |                                                                  |
|-------------------------|------------------------------------------------------------------|
| <b>Refresh interval</b> | Set how often the web-based manager updates the SMC status page. |
| <b>Go</b>               | Set the selected refresh interval.                               |
| <b>Refresh</b>          | Manually update the SMC status page.                             |
| <b>SMC#</b>             | Shelf manager card number: 1 or 2.                               |
| <b>Status</b>           | Current status of this shelf manager card.                       |
| <b>Refresh</b>          | Select to manually update the chassis status display.            |
| <b>Active/Standby</b>   | Mode of this shelf manager card: Active or Standby.              |

## Node cards

In **System > Chassis > Node Cards**, you can reset blade units, and monitor temperature and voltage for each blade unit. In the Node Card list, the following displays:

|                         |                                                                               |
|-------------------------|-------------------------------------------------------------------------------|
| <b>Reset</b>            | Select to reset the selected blade units.                                     |
| <b>Refresh Interval</b> | Select to control how often the web-based manager updates the status display. |
| <b>Go</b>               | Select to set the selected automatic refresh interval.                        |
| <b>Refresh</b>          | Select to manually update the chassis status display.                         |
| <b>Selection</b>        | Enable to include blade in Reset action.                                      |
| <b>Blade #</b>          | Blade unit number. The unit number where connected is shown in bold.          |
| <b>Temperature</b>      | The temperatures according to sensors on the blade unit.                      |
| <b>Voltage</b>          | The voltages on the blade unit busses.                                        |

## Switch cards

From **System > Chassis > Switch Cards**, you can monitor temperatures and voltages for each switch card.

|                         |                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------|
| <b>Reset</b>            | Select to reset the selected blade units.                                           |
| <b>Refresh Interval</b> | Select to control how often the web-based manager updates the blade status display. |
| <b>Go</b>               | Select to set the selected automatic refresh interval.                              |
| <b>Selection</b>        | Enable to include blade in Reset action.                                            |
| <b>Blade #</b>          | Switch unit number.                                                                 |
| <b>Temperature</b>      | The temperature according to sensors on the blade unit.                             |
| <b>Voltage</b>          | The voltages on the switch unit busses.                                             |

## Chassis status – FortiGate-4000

The following is information about chassis status on the FortiGate-4000 units.

### Chassis status

You can monitor temperatures, voltages and cooling fan speeds. The following is displayed when monitoring temperatures, voltages and cooling fan speeds.

|                         |                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------|
| <b>Refresh interval</b> | Select to control how often the web-based manager updates the system status display. |
| <b>Go</b>               | Select to set the selected automatic refresh interval.                               |
| <b>Refresh</b>          | Select to manually update the chassis status display.                                |
| <b>Fan Speed</b>        | Fan speed for each chassis cooling fan or N/A if a fan is not installed.             |
| <b>Temperature</b>      | Temperature at each chassis temperature sensor or N/A if a sensor is not installed.  |
| <b>Voltage</b>          | Voltage on each power supply bus.                                                    |

The reported values are color coded. Green indicates the value is in the normal range. Yellow is a warning and red indicates that the value is critically out-of-range.

## Blade status

You can monitor fan speed, temperature and voltage for each blade unit. You can switch blade units on or off and control which blade unit's management interface is available through the KVM switch.

|                         |                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Power Up</b>         | Select to power up the selected blade units.                                                                                                                  |
| <b>Power Down</b>       | Select to power down the selected blade units.                                                                                                                |
| <b>Reset</b>            | Select to reset the selected blade units.                                                                                                                     |
| <b>Refresh interval</b> | Select to control how often the web-based manager updates the blade status display.                                                                           |
| <b>Go</b>               | Select to set the selected automatic refresh interval.                                                                                                        |
| <b>Set KVM</b>          | Select to set the KVM switch to the management interface of the selected blade unit. Select only one blade unit.                                              |
| <b>Refresh</b>          | Select to manually update the chassis status display.<br>If you want, select the check box to include blade in Power Up, Power Down, Reset or Set KVM action. |
| <b>Blade #</b>          | Blade unit number. The unit number where connected is shown in bold.                                                                                          |
| <b>Status</b>           | The status of the blade unit: On, Off, or N/Popul if no unit is present.                                                                                      |
| <b>Fan Speed</b>        | The speed of the blade unit fan.                                                                                                                              |
| <b>Temperature</b>      | The temperature of the blade unit.                                                                                                                            |
| <b>Voltage</b>          | The blade unit voltage.                                                                                                                                       |
| <b>KVM</b>              | A checkmark icon indicates that the KVM switch has selected the blade unit's management interface.                                                            |

### To power up or power down FortiGate blades

- 1 Enable the check box for the unit or units you want to control.
- 2 Select Power Up or Power Down as required.

### To reset FortiBlade units

- 1 Enable the checkbox for the unit or units to reset.
- 2 Select Reset.

### To select FortiBlade units for console access

- 1 Enable the check box for a unit.  
Select only one unit for console access.
- 2 Select Set KVM.

### Out of band management

From **System > Chassis > OOB Management**, you can configure the out of band management interface for the FortiGate-4000 unit. This feature enables you to set the out of band management IP address of the FortiGate-4000 unit, including changing the default route for this interface, and control administrative access connection to the out of band management interface.

This feature is available in both Transparent and NAT/Route mode.

The out of band management interface displays the following:

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Interface</b>             | The MAC address of the OOB Management interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>IP/Netmask</b>            | The OOB Management IP address. Enter an IP address and netmask that is valid for the network where you want to manage the FortiGate unit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Administrative Access</b> | Select the administrative access methods for the out of band management interface. <ul style="list-style-type: none"> <li><b>HTTPS</b> Allow secure HTTPS connections to the web-based manager through this interface.</li> <li><b>PING</b> Allow this interface to respond to pings. Use this setting to verify your installation and for testing.</li> <li><b>HTTP</b> Allow HTTP connections to the web-based manager through this interface. HTTP connections are not secure and can be intercepted by a third party.</li> <li><b>SSH</b> To allow SSH connections to the CLI through this interface.</li> </ul> |
| <b>MTU</b>                   | Select Override default MTU value (1500) and enter the maximum packet size to change the MTU.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Route</b>                 | Enter routing information if your network requires it. <ul style="list-style-type: none"> <li><b>Destinati on IP/Mask</b> Enter the destination network IP and netmask if needed.</li> <li><b>Gateway</b> Enter the default gateway IP address if required.</li> <li><b>Distance</b> Enter the administrative distance or accept the default.</li> </ul>                                                                                                                                                                                                                                                             |

## Firewall

The firewall protection profile Spam filtering now uses the FortiGuard functionality; however, FortiShield is now FortiGuard.

## VPN

The following describes corrections to documentation for VPN.

### Updates to Phase 1 Peer Options documentation

The **VPN > IPSEC > Phase 1** in the web-based manager exhibits the following behavior when Authentication Method is set to Preshard key:

- When Remote Gateway is set to Static IP address, the only peer option presented is “Accept any peer ID” regardless of whether Mode is set to Aggressive or Main. The documentation incorrectly states that “Accept any peer ID” and “Accept peer ID” are available when Aggressive mode is selected.
- When Remote Gateway is set to Dialup User, the “Accept any peer ID”, “Accept this peer ID” and “Accept peer ID in dialup group” options are available regardless of whether Mode is set to Aggressive or Main. The documentation incorrectly states that when Main mode is selected, “Accept this peer ID” is not available.
- When Remote Gateway is set to Dynamic DNS, the “Accept any peer ID” and “Accept this peer ID” options are available regardless of whether Mode is set to Aggressive or Main. The documentation incorrectly states that when Main mode is selected, “Accept this peer ID” is not available.

### Phase 1 Peer ID used in dynamic DNS configurations

In a dynamic DNS configuration, one of the FortiGate units in a gateway-to-gateway configuration has a static domain name and dynamic IP address. During the Phase 1 exchange, a peer ID is used to establish the identity of the FortiGate unit that has a dynamic IP address. The *FortiGate Administration Guide* (MR10) incorrectly suggests that the peer ID should be a fully qualified domain name. In fact, the peer ID may be any character string, for example, a fully qualified domain name (FQDN).

The IP address of the FortiGate unit that has a static domain name may change at any time. Whenever the IP address changes, the tunnel is flushed and a new tunnel has to be established. The FortiGate unit that has a dynamic IP address may have to reconnect to establish a new VPN session. You can configure a ping server on the FortiGate unit that has a dynamic IP address to avoid a long interruption to traffic flow. Configure the ping server to ping a device on the network behind the FortiGate peer.

### Destination IP address for FortiClient dialup clients

When a dialup client connects to the Internet, an ISP typically assigns a dynamic IP address to the host of the VPN client through DHCP or PPPoE. You can choose whether to assign a virtual IP (VIP) address to the VPN client manually or through the FortiGate dialup server, via the DHCP relay.

If VIP addresses are configured manually, an exact VIP address or a subnet address comprising VIP addresses has to be specified in the firewall encryption policy destination address on the FortiGate dialup server. The FortiGate VPN Guide incorrectly states that the destination address may refer to a range of VIP addresses.

If VIP addresses are not assigned manually, or the FortiClient Acquire virtual IP address option is clear or the Acquire virtual IP address option is selected and the FortiClient Dynamic Host Configuration Protocol (DHCP) over IPsec option is selected, then the firewall encrypted policy destination address on the FortiGate dialup server must be set to “all”.

## VIP Addresses for the FortiClient dialup clients

When the FortiClient Host Security application is installed on a remote dialup host, the FortiGate dialup server may assign virtual IP (VIP) addresses to FortiClient VPN clients through DHCP relay.

Although the FortiGate VPN Guide states that you may assign VIP addresses that match the network behind the FortiGate dialup server, this type of configuration has the potential to create network overlap issues.

For example, the FortiClient host may be located in a remote office or hotel LAN, behind a NAT device. If the host device receives a private IP address from local DHCP server and then by co-incidence receives the same private IP address through FortiGate DHCP relay, a conflict will occur on the host dialup client's routing table and the FortiClient host will be unable to send traffic through the tunnel.

To determine which VIP address the FortiClient Host Security application is using in the CLI, type `ipconfig/all` at the Windows Command Prompt on the FortiClient host. The output will also show the IP address that has been assigned to the host Network Interface Card (NIC).

If you want to use VIP addresses and avoid network overlap issues in this type of situation, assigns VIP addresses from a subnet address that is not commonly used. For example, 10.254.254.0/24 or 192.168.254.0/24.

## Dialup server mode of operation

When a FortiClient dialup client establishes a tunnel with a FortiGate dialup server, the following occurs:

- The Remote Gateway column in the VPN dialup monitor displays either the public IP address and UDP port of the remote host device, on which the FortiClient Host Security application is installed, or if a NAT device exists in front of the remote host the public IP address and UDP port of the remote host.
- If VIP addresses are not used and the remote host connects to the Internet directly, the Proxy ID Destination column displays the public IP address of the Network Interface Card (NIC) in the remote host.
- If VIP addresses are not used and the remote host is behind a NAT device, the Proxy ID Destination column displays the private IP address of the NIC in the remote host.
- If VIP addresses were configured manually or through the FortiGate DHCP relay, the Proxy ID Destination column displays a specific Virtual IP (VIP) address belonging to a FortiClient dialup client, or a subnet address comprising VIP addresses.

## Support for FortiGate dialup clients

A dialup client may be a FortiGate unit. See the *FortiGate VPN Guide* for more information on how to configure a FortiGate unit as a dialup client including infrastructure requirements.

The following is a general summary of FortiGate dialup client configuration:

- The FortiGate dialup client and the FortiGate dialup server may operate in NAT/Route mode or Transparent mode.

- When you define the Phase 1 settings on the FortiGate dialup client, specify a Local ID value under Advanced settings for the FortiGate dialup client to identify itself to the FortiGate dialup server. When you define the Phase 1 settings on the FortiGate dialup server, select Accept this peer ID under Peer Options, and enter the local ID value that you assigned to the FortiGate dialup client.
- Do not select DHCP-IPSec Enable in the Phase 2 Advanced settings on FortiGate dialup clients -- computers on the private network behind the FortiGate dialup client will most likely obtain IP addresses directly from a local DHCP server behind the FortiGate dialup client.
- When you define the firewall encryption policy on the FortiGate dialup server, the destination address must refer the private network behind the FortiGate dialup client.

After a tunnel with a FortiGate dialup client has been established, the VPN enables communications between the local remote private number as if a gateway-to-gateway configuration were in place. In the VPN dialup monitor on the FortiGate dialup server, the Remote Gateway column displays the public IP address and UDP port of the FortiGate dialup client. In addition, the Proxy ID Destination column displays the IP address of the remote private network.

## IPS

The following table describes revised IPS actions on signatures.

**Table 22: Actions to select for each predefined signature**

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Pass</b>         | When a packet triggers a signature, the FortiGate unit generates an alert and allows the packets through the firewall without further action. If logging is disabled and action is set to Pass, the signature is effectively disabled.                                                                                                                                                                                                                                    |
| <b>Drop</b>         | When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The firewall session is not touched. Fortinet recommends using an action other than Drop for TCP connection based attacks.                                                                                                                                                                                                                                                |
| <b>Reset</b>        | When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to both the client and server and drops the firewall session from the firewall session table.<br>This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session. |
| <b>Reset Client</b> | When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the client and drops the firewall session from the firewall session table.<br>This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.                 |
| <b>Reset Server</b> | When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the server and drops the firewall session from the firewall session table.<br>This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.                 |
| <b>Drop Session</b> | When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. For the remainder of this packet's firewall session, all follow-up packets are dropped.                                                                                                                                                                                                                                                                                   |

**Table 22: Actions to select for each predefined signature**

|                      |                                                                                                                                                                                                                                                                                                                                  |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Clear Session</b> | When a packet triggers a signature, the FortiGate unit generates an alert and the session to which the packet belongs is removed from the session table immediately. No reset is sent.<br>For TCP, all follow-up packets could be dropped.<br>For UDP, all follow-up packets could trigger the firewall to create a new session. |
| <b>Pass Session</b>  | When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall. For the remainder of this packet's session, the IPS is bypassed by all follow-up packets.                                                                                                                  |

The following are CLI commands relevant to IPS, including the command, `system autoupdate ips, new` for FortiOS 2.80MR10.

### **system autoupdate ips**

When IPS is updated, user-modified settings are retained. If the updated settings are different and if recommended IPS signature settings have not been modified, signature settings will be set according to the command `accept-recommended-settings`.

```
config sys autoupdate ips
 set accept-recommended-settings {enable | disable}
end
```

### **system global ips-open**

The IPS, if for any reason ceases to function, it will fail open by default. Network traffic will not be blocked and the Firewall continues to operate while the problem is being resolved.

```
config sys global
 set ip_signature {enable | disable}
end
```

### **system global ip\_siganture**

You can save system resources by restricting IPS processing to only those services allowed by firewall policies using the following command syntax pattern:

```
config sys global
 set ip_signatures {enable | disable}
end
```

### **system global ips-size**

You can set the size of the IPS buffer by using the following command syntax pattern:

```
config sys global
 set ips-size <ips_buffer_size>
end
```

## Antivirus

The following are new CLI commands for FortiOS 2.80MR10.

### system global av\_failopen

The Antivirus failopen is a safeguard feature that determines the behavior of the FortiGate antivirus system if it becomes overloaded in high traffic. The Antivirus failopen default is pass.

The antivirus system operates in one of two modes, depending on available memory. If the free memory is greater than 30 percent of the total memory, then the system is in non conservative mode. If the free memory drops to less than 20 percent of the total memory, then the system enters conserve mode. When the free memory once again reaches 30 percent or greater of the total memory, the system returns to non conserve mode.

See the [Antivirus failopen and optimization](#) article on the Fortinet Knowledge website for more information.

### system global optimize

The system global optimize feature configures CPU settings to ensure efficient operation of the FortiGate unit for either antivirus scanning or straight through traffic. When system global optimize is set to antivirus, the FortiGate unit uses symmetric multiprocessing to spread the antivirus tasks to server CPUs, enabling faster scanning.

For more information, see the [Antivirus failopen and optimization](#) article on the Fortinet Knowledge website.

## Web Filter

The category block configuration is changed and the cache for FortiGuard-Web filtering is enabled by default.

If you ordered FortiGuard-Web filtering through Fortinet technical support or are using the free 30-day trial, you only need to enable the service to start configuring and using FortiGuard-Web Filtering. You can configure category blocking from **Web Filter > Category Block > Configuration**. The FortiGuard-Web filtering settings displays on the Configuration page.

## Spam Filter

For FortiOS 2.80MR10, FortiShield Antispam is now called FortiGuard-Antispam Service. The name change applies throughout the Spam filter chapter of the FortiGate Administration Guide (MR10). The CLI command, `config spamfilter FortiShield`, is the same.

The cache for FortiGuard-Antispam is enabled by default.

If you ordered FortiGuard-Antispam Service through Fortinet technical support or are using the free 30-day trial, you only need to enable the service to start configuring and using FortiGuard-Antispam Service.

You can configure or view settings for the FortiGuard-Antispam Service by going to **Spam Filter > FortiGuard-AntiSpam**.

## New features and changes for FortiOS 2.80MR11

The following describes the new features and changes for FortiOS 2.80MR11 and includes some procedures for certain features. The following also includes corrections for errata in documentation.

### MTU Settings for VLAN subinterfaces

The MTU size for a VLAN subinterface is the same as the MTU of the physical interface. This size is no longer specified.

### Chassis status for FortiGate-5001 and FortiGate-5001FA2

The following is information about chassis status on the FortiGate-5001 and FortiGate-5001FA2.

#### SMC

You can check the status of your shelf manager cards by going to **System > Chassis > SMC** in the web-based manager. On the SMC page, the following displays:

|                         |                                                                  |
|-------------------------|------------------------------------------------------------------|
| <b>Refresh interval</b> | Set how often the web-based manager updates the SMC status page. |
| <b>Go</b>               | Set the selected refresh interval.                               |
| <b>Refresh</b>          | Manually update the SMC status page.                             |
| <b>SMC#</b>             | Shelf manager card number: 1 or 2.                               |
| <b>Status</b>           | Current status of this shelf manager card.                       |
| <b>Refresh</b>          | Select to manually update the chassis status display.            |
| <b>Active/Standby</b>   | Mode of this shelf manager card: Active or Standby.              |

#### Node cards

In **System > Chassis > Node Cards**, you can reset blade units, including monitor temperature and voltage for each blade unit. In the Node Card list, the following displays:

|                         |                                                                               |
|-------------------------|-------------------------------------------------------------------------------|
| <b>Reset</b>            | Select to reset the selected blade units.                                     |
| <b>Refresh Interval</b> | Select to control how often the web-based manager updates the status display. |
| <b>Go</b>               | Select to set the selected automatic refresh interval.                        |
| <b>Refresh</b>          | Select to manually update the chassis status display.                         |
| <b>Selection</b>        | Enable to include blade in Reset action.                                      |
| <b>Blade #</b>          | Blade unit number. The unit number where connected is shown in bold.          |
| <b>Temperature</b>      | The temperatures according to sensors on the blade unit.                      |
| <b>Voltage</b>          | The voltages on the blade unit busses.                                        |

#### Switch cards

From **System > Chassis > Switch Cards**, you can monitor temperatures and voltages for each switch card.

|                         |                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------|
| <b>Reset</b>            | Select to reset the selected blade units.                                           |
| <b>Refresh Interval</b> | Select to control how often the web-based manager updates the blade status display. |
| <b>Go</b>               | Select to set the selected automatic refresh interval.                              |
| <b>Selection</b>        | Enable to include blade in Reset action.                                            |
| <b>Blade #</b>          | Switch unit number.                                                                 |
| <b>Temperature</b>      | The temperature according to sensors on the blade unit.                             |
| <b>Voltage</b>          | The voltages on the switch unit busses.                                             |

## FortiGate 5001 blade configuration

The FortiGate 5001 blade is designed to work with the three FortiGate chassis: FortiGate-5050, FortiGate-5140, and FortiGate-5020. When a FortiGate 5001 blade is shipped, it is pre-configured with jumper settings for the type of chassis it will be going into. One setting is for chassis that have a shelf controller, such as the FortiGate-5050 and FortiGate-5140, and one if it does not, such as the FortiGate-5020.

The jumper setting can be incorrect if the wrong configuration was shipped to you, or if you upgrade your chassis from a FortiGate-5020 to a FortiGate-5050, or a FortiGate-5140. You need to change the jumper settings so that the FortiGate 5001 blade can communicate with the Shelf Manager.

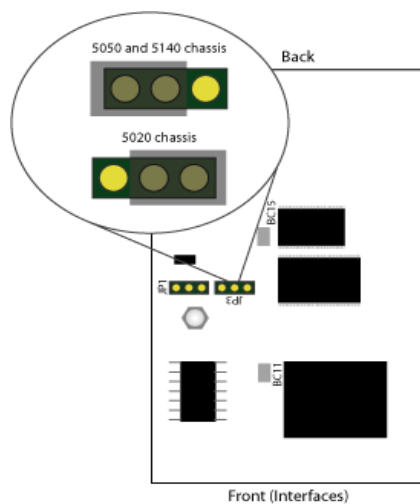


**Note:** The following procedure requires to manually change jumper settings on the FortiGate 5001 blade. Ensure that you are properly grounded before proceeding.

### To change the jumpers

- 1 Remove the FortiGate 5001 blade from the chassis.
- 2 Use the diagram below to locate the jumper settings on the left-hand side of the blade when the front (port interfaces) are facing you.
- 3 Carefully remove and place the jumper to the correct setting.
- 4 Place the blade back in the chassis.

**Figure 9: Jumper settings on the FortiGate 5001 blade**



## Firewall

The following describes the new features and changes to the Firewall menu from FortiOS 2.80MR8 to FortiOS 2.80MR10, including supplements to the Firewall chapter of the FortiGate Administration Guide for 2.80MR8.

### SMTP virus scanning only operates in splice mode

SMTP virus scanning operates in splice mode only. Splice mode is also called streaming mode. In splice mode, the FortiGate unit simultaneously scans an email and sends it to the SMTP server. If the FortiGate unit detects a virus, it terminates the server connection and returns an error message to the sender, listing the virus name and system generated quarantine file name. If SMTP quarantine is not enabled, the quarantine filename is blank. The SMTP server is not able to deliver the email if it was sent with an infected attachment. An error message is returned to the sender if an attachment is infected. The receive does not receive the email or the attachment.

### Spam filter email tagging for SMTP is not supported

The FortiGate unit discards spam email and immediately drops the connection because SMTP virus scanning operates in splice mode. In the US Domestic distribution, spam filter email tagging is not supported.

### SMTP quarantine file name system generated

When the FortiGate quarantines files from an SMTP email, the file name of the quarantined file is changed to a system generated file name. The system generated file name consists of the name of the sender email address and the name of the receiver email address separated with an underscore. The system generated file name does not include a file name extension.

For example, if the file test.doc was quarantined in an email being sent from user@address.com to info@fortinet.com the file name of the quarantined file would be user\_info.

### The default mail virus replacement message (splice mode)

The default mail virus message (splice mode) replacement message is changed.

|                                                                                          |                                                                           |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>From:</b>                                                                             | <b>To:</b>                                                                |
| %%FILE%% has been infected with the virus %%VIRUS%% File quarantined as %%QUARFILENAME%% | An email has been infected with the virus %%VIRUS%% File %%QUARFILENAME%% |

This change removes the name of the infected file from the replacement message. The replacement message now only contains the name of the virus that the file is infected with, including the quarantine filename.

For SMTP email %%QUARFILENAME%% is the system-generated quarantine file name. For other email protocols, %%QUARFILENAME%% is the original file name if quarantine is not enabled for the email protocol, and %%QYARFILENAME%% will be blank.

The %%FILE%% variables is still available. If you add %%FILE%% to the mail virus message (splice mode) replacement message. %%FILE%% will always add <no filename> to the replacement messages generated for viruses found in SMTP email. For other email protocols, %%FILE%% adds the name of the infected file to the replacement message.

## VPN Tunnel description update

The following is an update to a VPN Tunnel description. See the “Defining a firewall encryption policy” chapter of the *FortiGate IPSec VPN User Guide* for FortiOS 2.80MR11 for more information.

In the VPN menu, select a VPN tunnel for an ECRYPT policy. You can select an AutoIKE key or Manual Key tunnel.

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Allow Inbound</b>  | Select to enable traffic from a dialup client or computers on the remote private network to initiate the tunnel.                                                                                                                                                                                                                                                                                                                                             |
| <b>Allow Outbound</b> | Select to enable traffic from computers on the local private network to initiate the tunnel.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Inbound NAT</b>    | Select to translate the source IP addresses of inbound decrypted packets into the IP address of the FortiGate interface to the local private network.                                                                                                                                                                                                                                                                                                        |
| <b>Outbound NAT</b>   | Select in combination with a natip CLI value to translate the source addresses of outbound cleartext packets into the IP addresses that you specify. Do not select Outbound NAT unless you specify a natip value through the CLI. When a natip value is specified, the source addresses of outbound IP packets are replaced before the packets are sent through the tunnel. For more information, see the “firewall” chapter of the FortiGate CLI Reference. |

## Subnet specified for IP pool correction

The *FortiGate Administration Guide* (MR11) states that the IP address range defined for an IP pool must be on the same subnet as the IP address of the interface that you are adding the IP pool to. This is incorrect. The start and end of the range does not need to be on the same subnet as the IP address of the interface that you are adding the IP pool to.

## Mark as clear Spam Action correction

The *FortiGate Administration Guide* (MR11) states that when an antispam IP address, email address, MIME header, or banned word is set to ‘Mark as Clear’, the message containing a match is passed to the next filter. This is incorrect. When an antispam filter matches an IP address, email address, MIME header or banned word set to ‘Mark as Clear’, the message is exempt from the remaining spam filters.

## System Interface CLI command: forward\_domain

The following CLI command is used to separate interfaces into separate collision domains. The forward\_domain command is an interface configuration subcommand and is only available in Transparent mode.

## Firewall CLI Commands

The command descriptions in the following table replace existing information in the Firewall Policy chapter of the FortiGate Command Line Interface Guide (MR11).

| Keywords and variables                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Default              | Availability                                                                       |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------|
| <code>dstaddr &lt;name_str&gt;</code>                                       | Enter the destination address for the policy. For a NAT policy you can also add a virtual IP. <code>name_str</code> is case sensitive.<br><br>If <code>action</code> is set to <code>encrypt</code> , enter the name of the IP address to which IP packets may be delivered at the remote end of the IPsec VPN tunnel. For details, see "Defining IP source and destination addresses" in the <i>FortiGate IPsec VPN User Guide</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | No default.          | All models.                                                                        |
| <code>inbound</code><br>{ <code>disable</code>   <code>enable</code> }      | When <code>action</code> is set to <code>encrypt</code> , enable or disable traffic from computers on the remote private network to initiate an IPsec VPN tunnel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <code>enable</code>  | All models.<br><code>action</code><br><code>encrypt</code><br>only                 |
| <code>nat inbound</code><br>{ <code>disable</code>   <code>enable</code> }  | When <code>action</code> is set to <code>encrypt</code> , enable or disable translating the source address IP packets emerging from the tunnel into the IP address of the FortiGate interface to the local private network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <code>disable</code> | All models.<br><code>action</code><br><code>encrypt</code><br>only                 |
| <code>natip</code><br>< <code>address_ipv4 mask</code> >                    | When <code>action</code> is set to <code>encrypt</code> and <code>nat outbound</code> is enabled, specify the source IP address and subnet mask to apply to outbound cleartext packets before they are sent through the tunnel.<br><br>If you do not specify a <code>natip</code> value when <code>nat outbound</code> is enabled, the source addresses of outbound encrypted packets are translated into the IP address of the FortiGate external interface. When a <code>natip</code> value is specified, the FortiGate unit uses a static subnetwork-to-subnetwork mapping scheme to translate the source addresses of outbound IP packets into corresponding IP addresses on the subnetwork that you specify. For example, if the source address in the firewall encryption policy is 192.168.1.0/24 and the <code>natip</code> value is 172.16.2.0/24, a source address of 192.168.1.7 will be translated to 172.16.2.7 | 0.0.0.0<br>0.0.0.0   | All models.<br><code>Encrypt</code><br>policy, with<br>outbound<br>NAT<br>enabled. |
| <code>nat outbound</code><br>{ <code>disable</code>   <code>enable</code> } | When <code>action</code> is set to <code>encrypt</code> , enable or disable translating the source addresses of outbound encrypted packets into the IP address of the FortiGate outbound interface. Enable this attribute in combination with the <code>natip</code> attribute to change the source addresses of IP packets before they go into the tunnel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <code>disable</code> | All models.<br><code>action</code><br><code>encrypt</code><br>only                 |

|                                |                                                                                                                                                                                           |             |                                          |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------------------------|
| outbound<br>{disable   enable} | When action is set to encrypt, enable or disable traffic from computers on the local private network to initiate an IPSec VPN tunnel.                                                     | enable      | All models.<br>action<br>encrypt<br>only |
| srcaddr <name_str>             | Enter the source address for the policy. name_str is case-sensitive. If action is set to encrypt, enter the private IP address of the host, server, or network behind the FortiGate unit. | No default. | All models.                              |
| vpntunnel<br><name_str>        | When action is set to encrypt, enter the name of the IPSec tunnel that will be subject to this firewall encryption policy.                                                                | No default. | All models.<br>action<br>encrypt<br>only |

## SIP

This CLI command is new for FortiOS 2.80MR10. The Session Initiation Protocol (SIP) is a predefined service.

| Service name | Description                                                                                           | Protocol | Port |
|--------------|-------------------------------------------------------------------------------------------------------|----------|------|
| SIP          | Session Initiation Protocol defines how audiovisual conferencing data is transmitted across networks. | udp      | 5060 |

## IPSec VPN

It is recommended to review the revised version of the FortiGate VPN Guide available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following are Phase 1 basic setting options when configuring a new VPN gateway in FortiOS 2.80MR11.

- Gateway Name** Enter the name that reflects the origination of the remote connection.
- Remote Gateway** Select the nature of the remote connection:
- If a remote peer with a static IP address will be connecting to the FortiGate unit, select Static IP address.
  - If one or more FortiGate/FortiClient dialup clients with dynamic IP addresses will be connecting to the FortiGate unit, select Dialup User.
  - If a remote peer that has a domain name and subscribes to a dynamic DNS service will be connecting to a FortiGate unit, select Dynamic DNS.
- IP Address** If you set Remote Gateway to Static IP Address, type the IP address of the remote peer.
- Dynamic DNS** If you set Remote Gateway to Dynamic DNS, type the domain name of the remote peer.
- Mode** Select Main or Aggressive, depending on the Peer Options setting.
- In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.
  - In Aggressive mode, the phase1 parameters are exchanged in single message with authentication information that is not encrypted. You must select Aggressive when the remote FortiGate unit has a dynamic IP address.
- Authentication Method** Select Pre-shared Key or RSA Signature.
- Pre-shared Key** If Pre-shared Key is selected, type the preshared key that the FortiGate unit will use to authenticate itself to the remote peer or client during phase 1 negotiations. You must define the same value at the remote peer or client. The key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.
- Certificate Name** If RSA Signature is selected, select the name of the server certificate that the FortiGate unit will use to authenticate itself to the remote peer or client during phase 1 negotiations.

**Peer Options**

To accept connections without checking peer IDs, select Accept any peer ID.

To grant access to one or more remote peers or FortiGate dialup clients based on a peer ID, select Accept this peer ID and type the identifier. This value must be identical to the value in the Local ID field of the phase 1 remote gateway configuration on the remote peer or FortiGate dialup client. If you are configuring authentication parameters for FortiClient dialup clients, refer to the Authentication FortiClient Dialup Clients Technical Note.

To grant access to dialup users based on the name of the dialup group, select Accept peer ID in dialup group and select the name of the group from the list. You must create the user group before it can be selected here. See the "User" chapter of the FortiGate Administration Guide (MR11).

To authenticate one or more remote peers or dialup clients based on a particular or shared security certificate, select Accept this peer certificate only and select the name of the certificate from the list. The certificate must be added to the FortiGate configuration through the config user peer CLI command before it can be selected here. For more information, see the "config user" chapter of the FortiGate CLI Reference Guide. If the remote VPN peer or client has a dynamic IP address, set Mode to Aggressive.

Select Accept this peer certificate group only to use a certificate group to authenticate remote peers and dialup clients that have dynamic IP addresses and use unique certificates. Select the name of the group from the list. The group must be added to the FortiGate configuration through the config user peer and config user peergrp CLI commands before it can be selected here. For more information, see the "config user" chapter of the FortiGate CLI Reference Guide. When the remote peers and clients have dynamic IP addresses, you must set Mode to Aggressive.

**Advanced**

You may retain the default settings unless changes are needed to meet your specific requirements.

## Phase 1 advanced settings

The following are Phase 1 advanced settings.

- Local ID**      If the FortiGate unit will act as a VPN client and you are using peer IDs for authentication purposes, enter the identifier that the FortiGate unit will supply to the VPN server during the phase 1 exchange.  
 If the FortiGate unit will act as a VPN client and you are using security certificates for authentication, select the distinguished name (DN) of the local server certificate that the FortiGate unit will use for authentication purposes.  
 If the FortiGate unit is a dialup client and will not be sharing a tunnel with other dialup clients, that is the tunnel will be dedicated to this FortiGate dialup client, set Mode to Aggressive.
- XAuth**      If you select Enable as Client, type the user name and password that the FortiGate unit will need to authenticate itself to the remote peer.  
 To select Enable as Server, you must first create user groups to identify the dialup clients that need access to the network behind the FortiGate unit. You must also configure the FortiGate unit to forward authentication requests to an external RADIUS or LDAP authentication server. For information about these topics, see the “Users and Authentication” chapter of the FortiGate Administration Guide. Select a Server Type setting to determine the type of encryption method to use between the FortiGate unit, the XAuth client and the external authentication server, and then select the user group from the User Group list.

## Phase 2 advanced options

The following are Phase 2 advanced options settings.

- DHCP-IPSec**      Select Enable if the FortiGate unit acts as a dialup server and FortiGate DHCP relay will be used to assign VIP addresses to FortiClient dialup clients. So not select this option on FortiGate units that act as dialup clients. The DHCP relay parameters must be configured separately.
- Internet browsing**      Select the FortiGate interface to the local private network if the FortiGate e unit has to support an Internet-browsing configuration. Do not select this option on FortiGate units that act as dialup clients.

## Dialup monitor

The following is displayed in the Dialup monitor section of the IPsec VPN Monitor page.

**Remote gateway**

The meaning of the value in the Remote gateway column changes, depending on the configuration of the network at the far end:

- When a FortiClient dialup client establishes a tunnel, the Remote gateway column displays either the public IP address and UDP port of the remote host device, on which the FortiClient Host Security application is installed, or if a NAT device exists in front of the remote host, the Remote gateway column displays the public IP address and UDP port of the remote host.
- When a FortiGate dialup client establishes a tunnel, the Remote gateway column displays the public IP address and UDP port of the FortiGate dialup client.

**Proxy ID Destination**

The meaning of the value in the Proxy ID Destination column changes, depending on the configuration of the network at the far end.

When a FortiClient dialup client establishes a tunnel:

- If VIP addresses are not used and the remote host connects to the Internet directly, the Proxy ID Destination field displays the public IP address of the Network Interface Card (NIC) in the remote host.
- If VIP addresses are not used and remote host is behind a NAT device, the Proxy ID Destination field displays the private IP address of the NIC in the remote host.
- If VIP addresses were configured, manually or through FortiGate DHCP relay, the Proxy ID Destination field displays either the CIP address belonging to a FortiClient dialup client, or a subnet address from which VIP addresses were assigned.

When a FortiGate dialup client establishes a tunnel, the Proxy ID Destination field displays the IP address of the remote private network.

**config vpn ipsec phase 1**

The following description of the IPsec Phase 1 `localid` attribute should be updated as in the table below.

| Keywords and variables                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Default    | Availability |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------|
| <code>localid</code><br><code>&lt;id_str&gt;</code> | Enter a local ID if the FortiGate unit is functioning as a VPN client and will use the local ID for authentication purposes. If you want to dedicate a tunnel to a FortiGate dialup client, you must assign a unique identifier (local ID) to the FortiGate client. Whenever, you configure a unique identifier (local ID) on a FortiGate dialup client, you must enable aggressive mode on the FortiGate dialup sever and also specify the identifier as a peer ID on the FortiGate dialup server. | No default | All models.  |

**config vpn ipsec phase 2**

The following description of the IPsec Phase 2 `dhcp-ipsec` and `intenetbrowsing` attributes should be updated as in the table below.

| Keywords and variables                   | Description                                                                                                                                                                                                                                                                                                                                                | Default    | Availability                                                       |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|--------------------------------------------------------------------|
| dhcp-ipsec<br>{disable   enable}         | Enable or disable FortiGate DHCP relay. If the FortiGate unit acts as a dialup server and FortiGate DHCP relay will be used to assign VIP addresses to FortiClient dialup clients, enable the attribute. Leave the attribute disabled on FortiGate units that act as dialup clients. The FortiGate unit can relay the requests to an external DHCP server. | disable    | All models.<br>phase1name must name a dialup gateway configuration |
| internetbrowsing<br><interface-name_str> | Enter the name of the FortiGate interface to the local private network if the FortiGate unit has to support an Internet-browsing configuration. Do not set this attribute on FortiGate units that act as dialup clients.                                                                                                                                   | No default | All models.                                                        |

## Spam Filter

The order of incoming mail passed through the FortiGate spam filter is determined by the protocol used to transfer the mail. The order is as follows:

### For SMTP

- 1 IP address BWL check -- Last hop IP
- 2 RBL & ORDBL check IP address FortiShield check, HELO DNS loop
- 3 Email address BWL check
- 4 MIME headers check
- 5 IP address BWL check (for IPs extracted from "Received" headers)
- 6 Return email DNS check, FortiGuard Antispam check (for IPs extracted from "Received" headers, and URLs in email content)
- 7 Banned word check

### For POP3 and IMAP

- 1 Email address BWL check
- 2 MIME headers check, IP BWL check
- 3 Return e-mail DNS check, FortiGuard Antispam check, RBL & ORDBL check
- 4 Banned word check

### For SMTP, POP3, and IMAP

Filters requiring a query to a server and a reply (FortiGuard Antispam Service and DNSBL/ORDBL) are run simultaneously. To avoid delays, queries are sent while other filters are running. The first reply to trigger a spam action takes effect as soon as the reply is received.



# Upgrading to FortiOS 2.80

Before you begin upgrading to FortiOS 2.80, it is recommended that you first review this chapter as well as the release notes so you can be fully aware of these new features and changes.

It is recommended to upgrade to FortiOS 2.5MR10 before upgrading to FortiOS 2.80MR4 and higher. The following describes upgrading from FortiOS 2.50MR10 to FortiOS 2.80MR11. If your FortiGate unit already has FortiOS 2.80, it is recommended to upgrade to at least FortiOS 2.80MR5 before upgrading to FortiOS 2.80MR8 or higher.

This chapter includes the following sections:

- [Backing up your configuration](#)
- [Testing FortiOS 2.80 before installing it](#)
- [Upgrading your FortiGate unit](#)
- [Verifying the upgrade](#)
- [Converting your replacement messages to FortiOS 2.80](#)
- [Upgrading to FortiOS 2.80 using the FortiManager System](#)
- [Upgrading FortiOS 2.80 firmware releases](#)

## Backing up your configuration

Fortinet recommends that you back up all configuration settings from your FortiGate unit(s) before upgrading to FortiOS 2.50. It is recommended to back up FortiOS 2.50 replacement messages since these are not carried forward during the upgrade process.

Use the following procedures to backup your configuration file(s) and replacement messages for FortiOS 2.50 in either the web-based manager or the CLI.



**Note:** Always backup your configuration before upgrading to a current firmware version, or when resetting to factory defaults.

### Backing up your configuration using the web-based manager

Use the following procedure to backup your current configuration in the web-based manager.

#### To backup your configuration file using the web-based manager

- 1 Go to **System > Status > System Settings**.
- 2 Select Backup.
- 3 Select Backup system settings and save the configuration settings.
- 4 Select Return to return to the Status page.

## Backing up your configuration using the CLI

Use the following procedure to backup up your current configuration in the CLI.

### To backup your configuration file using the CLI

Enter the following to backup the configuration file.

```
execute backup <name_str> <tftp_ipv4>
```

Where <name\_str> is the name of the backup configuration file and <tftp\_ipv4> is the IP address of the TFTP server.

This may take a few minutes.

After successfully backing up your configuration file(s), either from the CLI or the web-based manager, proceed with backing up your replacement messages.

## Backing up your replacement messages

You need to backup your replacement messages since they are not carried forward. Use the following procedure to backup your replacement messages before upgrading to FortiOS 2.80.

### To backup your email virus messages replacement messages

- 1 Go to **System > Config > Replacement Messages**.
- 2 Open the Email Virus message replacement message.
- 3 Copy the message, "Sorry Dangerous Attachment has been Removed."
- 4 Open a text editing program, such as Notepad.
- 5 Paste the message and save the file.

Use the above procedure to backup all replacement messages. Go to ["Converting your replacement messages to FortiOS 2.80"](#) on page 79 after upgrading to FortiOS 2.80.

## Testing FortiOS 2.80 before installing it

It is recommended you test the firmware image before installing it onto your FortiGate unit. This enables you to familiarize yourself with the redesigned web-based manager and restructured CLI. When you test a firmware image, the image is installed onto system memory. If you reboot the system, the firmware image is deleted and you can install FortiOS 2.80 permanently.

For this procedure you:

- Access the CLI by connecting to the FortiGate console port using the serial cable
- Install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

### To test the firmware image

- 1 Connect to the CLI using the serial cable or console cable you received in your package contents for connecting to the CLI.
- 2 Make sure the TFTP server is running.

- 3 Copy the new firmware image file to the root directory of the TFTP server.
- 4 Ping to the TFTP server to verify the connection. For example, if the TFTP server's address is 192.168.168.1.168:
 

```
execute ping 192.168.168.1.168
```
- 5 Enter the following command to restart the FortiGate unit:
 

```
execute reboot
```

As the FortiGate unit reboots, press any key to interrupt the system startup. As the FortiGate unit starts, a series of system startup messages are displayed. When the following messages appears:

```
Press any key to display configuration menu.
...
```
- 6 Immediately press any key to interrupt the system startup.
 

If you successfully interrupt the startup process, the following message appears:

```
Enter the TFTP Server Address: [192.168.1.168]:
```
- 7 Type an IP address the FortiGate unit can use to connect to the TFTP server.
 

The IP address must be on the same network as the TFTP server, but make sure you do not use the IP address of another device on the network.

The following message appears:

```
Enter File Name [image.out]:
```
- 8 Enter the firmware image file name and press Enter:
 

The TFTP server uploads the firmware image file to the FortiGate unit and the following message appears:

```
Save as Default firmware/Run Image without saving:[D/R]?
```
- 9 Type R.
 

The firmware image is installed to system memory and the FortiGate unit starts running the new image but with its current configuration.

You can test the new firmware image as required.

### Verify the test firmware

You can verify the test firmware by logging into the web-based manager and going to **System > Unit Information > Firmware Version**, or using the following CLI command.

```
get system status
```

When you are ready to install FortiOS 2.80 permanently, reboot the FortiGate unit.

## Upgrading your FortiGate unit

You can upgrade to FortiOS 2.80 using either the web-based manager or CLI. However, it is recommended you upgrade using the CLI. Use the following procedures to upgrade your existing firmware version to FortiOS 2.80.

## Upgrading to FortiOS 2.80

This section describes the procedures for upgrading to FortiOS 2.80 using either the web-based manager or CLI.



**Note:** All configurations are lost when upgrading using the TFTP procedure


### Upgrading using the web-based manager

You can use the web-based manager to upgrade to FortiOS 2.80. Use the following procedure for upgrading to FortiOS 2.80.



**Note:** Before proceeding, make sure you back up your configuration. The upgrade installation process may take longer than other upgrade installations because the FortiGate unit reboots twice. The unit reboots once to install the firmware image and once to restore the configuration settings.

#### To upgrade to FortiOS 2.80 using the web-based manager

- 1 Copy the firmware image file to your management computer.
- 2 Log into the web-based manager.
- 3 Go to **System > Status**.
- 4 Select the Firmware Upgrade icon  .
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process may take a few minutes.

Once the upgrade is successfully installed:

- Ping to your FortiGate unit to verify there is still a connection.
- Clear the browser's cache and log into the web-based manager.



**Note:** After upgrading to FortiOS 2.80, perform an "Update Now" to retrieve the latest AV/NIDS signatures from the FortiProtect Distribution Network (FDN) as these signatures may be older than those currently available on the FDN.

### Upgrading using the CLI

Use the following procedures to upgrade to FortiOS 2.80 in the CLI.

#### To upgrade to FortiOS 2.80 using the CLI

- 1 Make sure the TFTP server is running.
- 2 Copy the new firmware image file to the root directory of the TFTP server.
- 3 Log into the CLI.
- 4 Ping to the TFTP server to verify the connection. For example, if the TFTP server's address is 192.168.168.1.168:

```
execute ping 192.168.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

```
execute restore image <name_str> <tftp_ip>
```

When `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is `192.168.1.168`, enter:

```
execute restore image.out 192.168.1.168
```

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

- 6 Reconnect to the CLI.
- 7 To confirm the firmware image is successfully installed, enter:

```
get system status
```

- 8 Update antivirus and attack definitions (see the *FortiGate Administration Guide* for your specific FortiGate unit), or from the CLI, enter:

```
execute update-now
```

## Verifying the upgrade

After logging back into the web-based manager, FortiOS 2.50 configuration settings are carried forward. For example, if you go to **Web Filter > Content Block** you can see your banned pattern list carried forward from your FortiOS 2.50 configuration settings.

Verifying your settings enables you to familiarize yourself with the new features and changes in FortiOS 2.80.

You can verify your configuration settings by:

- going through each menu and tab in the web-based manager
- using the `show shell` command in the CLI

## Converting your replacement messages to FortiOS 2.80

After successfully upgrading to FortiOS 2.80, you can convert your FortiOS 2.50 replacement messages to FortiOS 2.80 format. Use the following procedure to convert your replacement messages.

### To convert your replacement messages to FortiOS 2.80

- 1 Log into the CLI.
  - 2 Enter the following commands:
- ```
config system replacemsg mail email_virus
```
- 3 Open your saved text file with the replacement messages.
 - 4 Copy the email virus message "Sorry Dangerous Attachment has been Removed."
 - 5 In the CLI, enter the following command:
- ```
set buffer
```

- 6 Paste the message into the CLI.
- 7 Enter the following CLI command:

```
end
```

Use the above procedure to copy all FortiOS 2.50 replacement messages into the CLI. Make sure to back up your configuration file. This ensures these messages are now part of your FortiOS 2.80 configuration and are not lost if you require rebooting the system firewall or shutting down the unit.



**Note:** The operating system of the management computer should support the display of Japanese characters, if the replacement message contains Japanese characters. Encoding of web browser(s) on the management computer should be set to Japanese, if required.

## Upgrading to FortiOS 2.80 using the FortiManager System

If your FortiGate unit is connected to a FortiManager unit, you can upgrade the FortiGate unit to FortiOS 2.80 using the FortiManager System. However, there are some issues you need to know about upgrading your FortiGate unit using the FortiManager System.

When you upgrade to FortiOS 2.80 using the FortiManager System, you can ensure a successful upgrade by following these steps in the order they appear:

- Back up the FortiGate unit's FortiOS 2.50 configuration file.
- Transfer the FortiOS 2.80 firmware image to the FortiGate unit.
- Resynchronize the FortiGate unit.
- Format the FortiGate unit's log disk.
- Reconfigure the FortiGate unit.
- If required, configure the IPSec VPN between the FortiManager Server and the FortiGate unit.

Document all admin users, including any Transparent mode virtual domains, that are in your FortiOS 2.50 configuration. Only a certain number of admin users are carried forward in FortiOS 2.80 and only the first ten virtual domains are carried forward as well.

You can enable the IPSec tunnel from the FortiGate side because both the FortiManager Server 2.80 and FortiOS 2.80 have built-in VPN configuration. For the VPN tunnel to work properly, make sure the system date and time on both devices match. The FortiGate unit should be in the management virtual domain. Only the management virtual domain can initiate VPN traffic.

If you are transferring a firmware image to a FortiGate unit running FortiOS 2.50 and the transfer fails, you must reboot the FortiGate unit to release the flash memory before you can transfer the image again.

The following settings need to be reconfigured after upgrading to FortiOS 2.80 using the FortiManager System:

- RIP
- Policy routing
- NIDS (now called IPS in 2.80)
- Interface
- VLAN

- Policy
- Address and address group
- Zone
- Local user and user group

You will also need to format the FortiGate log disk if the FortiGate unit has a hard disk. However, formatting the disk will erase all quarantine file and logging data stored on the disk so back up all log data before formatting the FortiGate log disk.

## Upgrading FortiOS 2.80 firmware releases

If you have an earlier version of FortiOS 2.80, you should upgrade to at least FortiOS 2.80MR5 before upgrading to a higher version of FortiOS 2.80. It is recommended that you read the following before upgrading FortiOS 2.80 maintenance releases. There are several issues when upgrading in FortiOS 2.80.

If you are upgrading from FortiOS MR4 to FortiOS 2.80MR5, it is recommended to do the following:

- If you model has a hard disk, back up the log files then run `execute formatlog disk` from the CLI or accept the pop-up window prompt in the web-based manager after the first login. This operation erases any existing log files on the hard disk, requires several minutes to complete, and involves a system reboot. Backup the log files before executing this command and choose a low traffic period since there is a brief interruption while the unit reboots.

If you are upgrading from FortiOS 2.80MR7, including up to FortiOS 2.80MR10, it is recommended that you do the following:

Convert the stored configuration so that an internal re-write of the current configuration is preserved in memory. For example, go to the Edit screen for an address in the firewall policies, click OK to reapply the existing settings. This action forces an internal re-write of the configuration tables and ensures that they will be preserved. After an upgrade, the configuration stored on the non-volatile memory is still in the previous version format until a configuration change is made. Re-apply any existing setting in the current configuration to convert the configuration.

When upgrading from FortiOS 2.80MR6, FortiManager 2.80MR6 is supported. All FortiManager 2.80MR6 and up to FortiManager 2.80MR10 is supported with same FortiOS 2.80 firmware release. FortiOS 2.80MR11 and FortiOS 2.80MR12 both support FortiManager 3.0GA.

The following are issues you may encounter if you are upgrading FortiOS 2.80 firmware releases:

### FortiOS MR4 upgrading to FortiOS 2.80 MR5 to MR11

The Spam Filter List format was changed in FortiOS 2.80MR3 and restoring any old format lists will fail. Contact Customer support for assistance in converting pre-MR4 lists. Existing lists in the FortiGate configuration are converted as part of the firmware upgrade process.

The User Domain function for FortiOS 2.80MR2 and earlier has been removed from FortiOS 2.80MR3 and later releases. Any firewall policies that use User Domain will be deleted from the configuration when upgrading to FortiOS 2.80MR3. The User Domain function has been replaced by an expanded User Group function that allows a User Group to be associated with a protection profile.

To upgrade a HA cluster from a previous FortiOS 2.80 version, only the primary unit needs to be upgraded if the current version is FortiOS 2.80. The subordinate units will be automatically upgraded by the primary unit.

### FortiOS 2.80MR6 upgrading to FortiOS MR7 to MR11

Ensure that all protection profiles have the AV Buffer-To-Disk option disabled prior to upgrading from a pre-MR4 version. Failure to do so will result in all AV scanning options disabled in all protection profiles after the upgrade.

### FortiOS 2.80MR8 upgrading to FortiOS 2.80MR9 to MR11

When upgrading from FortiOS 2.80MR7, the IPSec Phase 1 Peer ID configuration is reset to "Accept any peer ID". This is a problem with FortiOS 2.80MR7 with the Peer ID setting saved incorrectly in the configuration in the non-volatile memory. FortiOS 2.80MR9 correctly saves the Peer ID settings.

When upgrading from FortiOS 2.80 MR6 or earlier, web pattern block entries that use certain special characters are removed from the configuration. This issue has been fixed. The special characters are < > ( ) # " ' .

In FortiOS 2.80MR9, newly added NAT VIPs do not work unless the configuration is rewritten prior to using it. For example,

- 1 configure static NAT VIP
- 2 add to firewall policy
- 3 re-apply any existing setting in the current configuration, such as a firewall address

The static NAT VIP will not work if the last step is skipped. Existing VIPs prior to upgrade are not affected.

## Upgrading using the web-based manager

The following enables you to upgrade to any FortiOS 2.80 maintenance release using the web-based manager. If your FortiGate unit already has FortiOS 2.80MR4 or earlier, it is recommended to upgrade to at least FortiOS 2.80MR5 before upgrading to a higher version of FortiOS 2.80.



**Note:** You must login using the admin administrator account, or an administrator account that has system configuration read and write privileges when using this procedure.



**Note:** Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After installing new firmware, update your antivirus and attack definitions using either the CLI command `execute update_now` or the web-based manager. See the FortiGate Administration Guide for more information.

**To upgrade using the web-based manager**

- 1 Copy the firmware image file to your management computer..
- 2 Log into the web-based manager as the admin administrative user.
- 3 Go to **System > Status**.
- 4 Select Update under **Unit Information > Firmware Version**.
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.  
The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.
- 7 Log into the web-based manager.
- 8 Go to **System > Status** and check the Firmware Version to confirm that the firmware upgrade is successfully installed.
- 9 Update antivirus and attack definitions. For information about updating antivirus and attack definitions, see your FortiGate Administration Guide for your specific FortiGate unit.

**Upgrading using the CLI**

The following enables you to upgrade to any FortiOS 2.80 maintenance release using the web-based manager. If your FortiGate unit already has FortiOS 2.80MR4 or earlier, it is recommended to upgrade to at least FortiOS 2.80MR5 before upgrading to a higher version of FortiOS 2.80.



**Note:** You must login using the admin administrator account , or an administrator account that has system configuration read and write privileges when using this procedure.



**Note:** Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After installing new firmware, update your antivirus and attack definitions using either the CLI command `execute update_now` or the web-based manager. See the FortiGate Administration Guide for more information.

**To upgrade using the CLI**

- 1 Copy the new firmware image file to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log into the CLI.
- 4 Enter the following command to ping the computer running the TFTP server. This ensures the FortiGate unit can connect to the TFTP server. For example, if the IP address of the TFTP 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

```
execute restore image <name_str> <tftp_ipv4>
```

Where <name\_str> is the name of the firmware image file and <tftp\_ip> is the IP address of the TFTP server. For example, if the firmware image file name is FGT\_300-v280-build183-FORTINET.out and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image FGT_300-v280-build183-FORTINET.out
192.168.1.168
```

- 6 The FortiGate unit responds with the following message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

- 7 Type *y*.

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version and restarts. This process takes a few minutes.

- 8 Reconnect to the CLI.

- 9 To confirm the new firmware image is successfully installed, enter:

```
get system status
```

- 10 Enter the following command to update antivirus and attack definitions:

```
execute update_now
```

See [“Testing FortiOS 2.80 before installing it” on page 76](#) for testing a firmware image before permanently installing it on your FortiGate unit.

## Install firmware from a system reboot using the CLI

This procedure installs a specified firmware image and resets the FortiGate unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware version.

For this procedure you:

- access the CLI by connecting to the FortiGate console port using a serial cable,
- installs a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, you should:

- back up the FortiGate unit configuration
- back up the IPS custom signatures
- back up web content and email filtering lists



**Note:** This procedure varies for different FortiGate BIOS versions. These variations are explained in the procedure steps that are affected. The version of the BIOS running on the FortiGate unit is displayed when you start the FortiGate unit using the CLI through a console connection.



**Note:** Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release you are installing. After installing new firmware, update your antivirus and attack definitions using either the CLI command `execute update_now` or the web-based manager. See the *FortiGate Administration Guide* for more information.

### To install firmware from a system reboot

- 1 Connect to the CLI using the serial cable and FortiGate console port.
- 2 Copy the new firmware image file to the root directory of the TFTP server.  
Ensure the internal interface is connected to the same network as the TFTP server.
- 3 Enter the following command to ping the computer running the TFTP server. This ensures the FortiGate unit can connect to the TFTP server. For example, if the IP address of the TFTP 192.168.1.168:

```
execute ping 192.168.1.168
```

- 4 Enter the following command to restart the FortiGate unit:

```
execute reboot
```

The FortiGate unit responds with the following message:

```
This operation will reboot the system!
Do you want to continue? (y/n)
```

- 5 Type `y`.

As the FortiGate unit starts, a series of system startup messages is displayed. When one of the following messages appears:

- FortiGate unit running v2.x BIOS

```
Press Any Key to Download Boot Image.
```

```
...
```

- FortiGate unit running v3.X BIOS

```
Press any key to display configuration menu
```

```
.....
```

Immediately press any key to interrupt the system startup. You have only three seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

- FortiGate unit running v2.x BIOS

```
Enter TFTP Server Address [192.168.1.168]:
```

Go to Step 7.

- FortiGate unit running v3.x BIOS

```
[G]: Get firmware image from TFTP server.
```

```
[F]: Format boot device.
```

```
[Q]: Quit menu and continue to boot with default firmware.
```

```
[H]: Display this list of options.
```

```
Enter G, F, B, Q, or H:
```

- 6 Type G to get the new firmware image from the TFTP server.  
The following message appears:  
Enter TFTP server address [192.168.1.168]:
- 7 Type the address of the TFTP server and press Enter.  
The following message appears:  
Enter Local Address [192.168.1.188]:
- 8 Type an IP address the FortiGate can use to connect to the TFTP server. The IP address can be any IP address that is valid for the network the interface is connected to. Make sure not to enter the IP address of another device on this network.  
The following message appears:  
Enter File Name [image.out]:
- 9 Enter the firmware image filename and press Enter.
- 10 The TFTP server uploads the firmware image file to the FortiGate unit and messages similar to the following are displayed:
  - FortiGate unit running v2.x BIOS  
Do You Want To Save The Image? [Y/n]  
Type Y.
  - FortiGate unit running v3.x BIOS  
Save as Default firmware/Run image without saving: [D/R]  
or  
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
- 11 Type D.
- 12 The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

# Reverting to FortiOS 2.50

You may need to revert to a previous firmware version if the upgrade did not install successfully. The following sections will help you to backup your current FortiOS 2.80 configuration, downgrade to FortiOS 2.50, and restore your FortiOS 2.50 configuration.

The following topics are included in this section:

- [Backing up your FortiOS 2.80 configuration](#)
- [Downgrading to FortiOS 2.50 using web-based manager](#)
- [Restoring your configuration](#)
- [Re-establishing connections](#)
- [Reverting to a previous FortiOS 2.80 firmware version](#)



**Note:** Before downgrading to FortiOS 2.50, or an earlier version of FortiOS 2.80, you will need to reformat the hard drive on FortiGate-200 units and above. The special hard drive formatting image requires uploading using the TFTP server procedure. See [“Downgrading to FortiOS 2.50 using the CLI” on page 88](#) for more information.

## Backing up your FortiOS 2.80 configuration

If you have configured additional settings in FortiOS 2.80, it is recommended you back up your FortiOS 2.80 configuration before downgrading to FortiOS 2.50. This ensures you have a current configuration file for FortiOS 2.80 if you decide to upgrade again.

Use the following procedure to backup your configuration onto your PC.



**Note:** Always backup your configuration before upgrading to a current firmware version, or when resetting to factory defaults.

### To backup your configuration to your management PC

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 Select the Backup icon to backup all configuration files.  
If you want, enter a password for the configuration file in the Password field and then select OK.
- 3 Select Apply.



**Note:** If you require to backup certain files, select the Backup icon that corresponds to each file.

## Downgrading to FortiOS 2.50 using web-based manager

Use the following procedure to downgrade to FortiOS 2.50 in the web-based manager. If you have created additional settings in FortiOS 2.80, make sure you back up your configuration before downgrading. See [“Backing up your FortiOS 2.80 configuration” on page 87](#) for more information.

### To downgrade using the web-based manager

- 1 Go to **System > Status > Firmware Version**.
- 2 Select Update.
- 3 Type the location of the firmware version or select Browse.
- 4 Select OK.

The following message appears:

- 5 Select OK.

The following message appears:

- 6 Select OK.

The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.

- 7 Log into the web-based manager.

Go to **System > Status** to verify the firmware version has changed to FortiOS 2.50.

### Verifying the downgrade

If you are unable to reconnect to your FortiGate unit, the internet or the web-based manager, see [“Re-establishing connections” on page 90](#) for more information.

### Downgrading to FortiOS 2.50 using the CLI

Use the following procedure to downgrade to FortiOS 2.50 in the CLI. If you have created additional settings in FortiOS 2.80, make sure you back up your configuration before downgrading. See [“Backing up your FortiOS 2.80 configuration” on page 87](#) for more information.

#### To downgrade using the CLI

- 1 Make sure the TFTP server is running.
- 2 Copy the firmware image file to the root directory of the TFTP server.
- 3 Log into the CLI.
- 4 Make sure the FortiGate unit can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

```
execute restore image tftp <name_str> <tftp_ipv4>
```

Where <name\_str> is the name of the firmware image file and <tftp\_ipv4> is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image tftp image.out
192.168.1.168
```

The FortiGate unit responds with the message:

```
This operation will replace the current firmware version! Do
you want to continue? (y/n)
```

**6** Type *y*.

The FortiGate unit uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

**7** Type *y*.

The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

**8** Reconnect to the CLI.

**9** To confirm the new firmware image has been loaded, enter:

```
get system status
```

See [“Restoring your configuration” on page 89](#) to restore your FortiOS 2.50 configuration settings.

## Restoring your configuration

The configuration settings for FortiOS 2.50 need to be restored after downgrading. During the downgrade process, most configurations revert to factory default settings.

### Restoring your configuration settings using the web-based manager

You can restore the FortiOS 2.50 configuration settings using the web-based manager. Use the following procedure to restore these settings.

#### To restore configuration settings using the web-based manager

- 1** Log into the web-based manager.
- 2** Go to **System > Status > System Settings**.
- 3** Select Restore.
- 4** Type the location of the file or select Browse to locate the file.
- 5** Select OK.

The FortiGate unit restores the configuration settings for FortiOS 2.50. This may take a few minutes.

To verify the configuration settings are restored, log into the web-based manager and go through the menus and tabs to verify the settings are restored.

## Restoring your configuration settings using the CLI

You can also restore the FortiOS 2.50 configuration settings using the CLI. Use the following procedure to restore these settings.

### To restore configuration settings using the CLI

- 1 Make sure the TFTP server is running.
- 2 Copy the backup configuration file to the root directory of the TFTP server.
- 3 Log into the CLI.
- 4 Ping to the TFTP server to verify the connection. For example, if the TFTP server's address is 192.168.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the backup configuration file to restore the file on the FortiGate unit:

```
execute restore config <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the backup configuration file and `<tftp_ipv4>` is the IP address of the TFTP server and `<passwd>` is the password you entered when you backup your configuration settings. For example, if the backup configuration file is `fgt.cfg` and the IP address of the TFTP server is 192.168.1.168:

```
execute restore config fgt.cfg 192.168.1.168
```

The FortiGate unit responds with the message:

```
This operation will overwrite the current settings!
Do you want to continue? (y/n)
```

- 6 Type `y`.

This may take a few minutes.

Use the `show shell` command to verify your settings are restored, or log into the web-based manager.

## Re-establishing connections

After downgrading to FortiOS 2.50, you may find some connections, such as connecting to the web-based manager or to the Internet, are lost. The following procedures help you to re-establish these connections.

### Re-establishing administrative access settings

Use the following procedure to re-establish administrative access settings when you are unable to connect to the web-based manager. You can also use the following procedure to re-establish administrative access settings for other interfaces.

**To enable Administrative Access settings to access the web-based manager**

- 1 Log into the CLI.
- 2 Enter the following command to display the administrative access settings for each interface:

```
show system interface
```

- 3 Enter the following commands to enable access to the web-based manager connection:

```
config system interface
 edit <interface_str>
 set allowaccess ping https http ssh
 end
```

- 4 Log into the web-based manager to verify the connection is successful.

You can use the above procedure for any interface you are unable to connect to. For example, if you are unable to connect to the CLI via an SSH connection, enable the SSH connection for your FortiGate unit's internal network interface.

**Re-establishing Internet connection**

If you are unable to connect to the Internet, use the following to re-establish this connection.

**To re-establish an Internet connection**

- 1 Ping to the external/public interface.  
If there is no ping, check if the allow access setting Ping is enabled.
- 2 Log into the web-based manager and check that the allow access HTTP setting is enabled for that interface.  
Enable the allow access HTTP setting if disabled.
- 3 If the allow access HTTP setting is enabled and no Internet connection can be established, reset the FortiGate unit to factory default settings and restore your configuration settings.



**Note:** Always backup your configuration before upgrading to a current firmware version, or when resetting to factory defaults.

**Reverting to a previous FortiOS 2.80 firmware version**

If an upgrade to a FortiOS 2.80 maintenance release is unsuccessful, you may want to revert to a previous FortiOS 2.80 firmware version instead of FortiOS 2.50. The following can be used for reverting to any FortiOS 2.80 firmware version.

**Reverting to a previous firmware version using the web-based manager**

The following procedures revert the FortiGate unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure you should do the following:

- back up the FortiGate unit configuration
- back up the IPS custom signatures
- back up web content and email filtering lists



**Note:** You must login using the admin administrator account , or an administrator account that has system configuration read and write privileges when you use this procedure.



**Note:** Installing firmware replaces the current antivirus and attack definitions along with the definitions included with the firmware release you are installing. After installing new firmware, make sure that antivirus and attack definitions are up to date. For more information, see the *FortiGate Administration Guide* for your specific FortiGate unit.

### To revert to a previous firmware version using the web-based manager

- 1 Copy the firmware image file to the management computer.
- 2 Log into the FortiGate web-based manager.
- 3 Go to **System > Status**.
- 4 Select Update under **Unit Information > Firmware Version**.
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.

The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.

- 7 Log into the web-based manager.
- 8 Go to **System > Status** and check the Firmware Version to confirm that the firmware is successfully installed.
- 9 Restore your configuration. See [“Restoring your configuration” on page 89](#).
- 10 Update antivirus and attack definitions. See your *FortiGate Administration Guide* specific to your FortiGate unit for more information.

### Reverting to a previous firmware version using the CLI

This procedure reverts the FortiGate unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure you can:

- Back up the FortiGate unit system configuration using the command `execute backup config`.
- Back up the IPS custom signatures using the command `execute backup ipsuserdefsig`
- Back up web content and email filtering lists.



**Note:** You must login using the admin administrator account , or an administrator account that has system configuration read and write privileges to use this procedure.



**Note:** Installing firmware replaces the current antivirus and attack definitions along with the definitions included with the firmware release you are installing. After installing new firmware, make sure that antivirus and attack definitions are up to date. For more information, see the *FortiGate Administration Guide* for your specific FortiGate unit.

### To revert to a previous firmware version using the CLI

- 1 Copy the firmware image file to the root directory of the TFTP server.
- 2 Start the TFTP server.
- 3 Log into the FortiGate CLI.
- 4 Enter the following command to ping the computer running the TFTP server. This ensures the FortiGate unit can connect to the TFTP server. For example, if the IP address of the TFTP 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

```
execute restore image <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `FGT_300-v280-build183-FORTINET.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image FGT_300-v280-build183-FORTINET.out
192.168.1.168
```

- 6 The FortiGate unit responds with the message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

- 7 Type `y`.

- 8 The FortiGate unit uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

```
Get image form tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

- 9 Type `y`.

The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

- 10 Reconnect to the CLI.
- 11 Enter the following to confirm that the new firmware image has been loaded:

```
get system status
```

- 12 Enter the following to restore your previous configuration, if needed:

```
execute restore config <name_str> <tftp_ipv4>
```

- 13 Update antivirus and attack definitions. See your *FortiGate Administration Guide* specific to your FortiGate unit for more information.



# Index

## Numerics

### 2.80MR11

- chassis status for FortiGate-5001 and FortiGate-5001FA2 65
- chassis status, Node Cards 65
- chassis status, SMC 65
- chassis status, Switch Cards 65
- config vpn ipsec phase 1 73
- default mail virus replacement message in splice mode 67
- dialup monitor 72
- Firewall 66
- firewall CLI commands 69
- FortiGate 5001 blade config 66
- IPSec VPN 70
- mark as clear spam action correction 68
- MTU settings for VLAN subinterfaces 65
- phase 1 advanced settings 72
- phase 2 advanced options 72
- SMTP quarantine file name system generated 67
- SMTP virus scanning only operates in splice mode 67
- Spam Filter 74
- spam filter email tagging for SMTP not supported 67
- subnet specified for IP pool correction 68
- system interface CLI forward\_domain 68
- VPN tunnel description update 68

### 2.80MR8 to 2.80MR10 51

- access profile prof\_admin 51
- alert message console 50
- Antivirus 63
- chassis status 57
- chassis status, blade status 58
- chassis status, FortiGate-4000 57
- chassis status, FortiGate-5000 56
- chassis status, Node Cards 57
- chassis status, out of band management 59
- chassis status, SMC 56
- chassis status, Switch Cards 57
- destination IP address for FortiClient dialup clients 60
- dialup server mode of operation 61
- Firewall 59
- FortiGate SNMP traps and fields 52
- FortiManager config 52
- IPS 62
- MIB fields 54
- phase 1 peer ID used in dynamic DNS config 60
- preventing public FortiGate interface from responding to ping requests 50
- Spam filter 64
- subordinate units block multicast and broadcast traffic in HA 51
- subordinate units logging and SNMP in HA 51
- support for FortiGate dialup clients 61
- system autoupdate ips 63
- system global av\_failopen 63

- system global ip\_signature 63
- system global ips-open 63
- system global ips-size 63
- system global optimize 64
- unit information 50
- updates to phase 1 peer options documentation 59
- updating MAC forwarding tables when link failover occurs, HA 51
- VIP addresses for FortiClient dialup clients 61
- VPN 59
- Web filter 64

## A

- access profile prof\_admin, 2.80MR8 to 2.80 MR10 51
- alert message console, 2.80MR8 to 2.80MR10 50
- antivirus menu
  - file block 41
- Antivirus, 2.80MR8 to 2.80MR10 63

## B

- backing up
  - 2.50 config using web-based manager 75
  - 2.50 configuration 75
  - 2.80 config 87
  - replacement messages 76
  - using the CLI 76
- backing up config files in 2.80 13
- blade status, 2.80MR8 2.80MR10 58

## C

- chassis status for FortiGate-5001 and FortiGate-5001FA2 65
- chassis status FortiGate-4000 59
- chassis status FortiGate-4000, 2.80MR8 to 2.80MR10 57
- chassis status FortiGate-5001 and FortiGate-5001FA2 65
- chassis status, FortiGate-4000 2.80MR8 to 2.80MR10 57
- chassis status, FortiGate-5000, 2.80MR8 to 2.80MR10 56
- CLI changes 17
- CLI command changes 30
- CLI commands
  - config vpn ipsec phase 1 73
  - firewall, 2.80MR11 69
  - system autoupdate ips 2.80MR8 to 2.80MR10 63
  - system global av\_failopen, 2.80MR8 to 2.80MR10 63
  - system global ip\_signature, 2.80MR8 to 2.80MR10 63
  - system global ips-open, 2.80MR8 to 2.80MR10 63
  - system global ips-size, 2.80MR8 to 2.80MR10 63
  - system global optimize, 2.80MR8 to 2.80MR10 64
- comments, documentation 11
- customer service 12

**D**

- default mail virus replacement message in splice mode, 2.80MR11 67
- destination IP address for FortiClient dialup clients, 2.80MR8 to 2.80MR10 60
- DHCP menu
  - dynamic IP 32
  - exclude range 32
  - IP/Mac binding 32
  - server 32
  - service 32
- dialup monitor, 2.80MR11 72
- dialup server mode of operation, 2.80MR8 to 2.80MR10 61
- documentation
  - commenting on 11
  - Fortinet 10
- downgrading
  - 2.50 using the CLI 88
  - to FortiOS 2.50 88
- downgrading in 2.80 using the CLI 92
- downgrading in 2.80 using the web-based manager 91
- downgrading to a previous 2.80 firmware version 91

**F**

- firewall CLI commands, 2.80MR11 69
- Firewall, 2.80MR11 66
- Firewall, 2.80MR8 to 2.80MR10 59
- FortiGate 5001 blade config
  - 2.80MR11 66
- FortiGate blade name change 14
- FortiGate documentation
  - commenting on 11
- FortiGate SNMP traps and fields, 2.80MR8 to 2.80MR10 52
- FortiGate-4000 chassis status 58
- FortiGate-5000 chassis status 56, 57
- FortiManager config, 2.80MR8 to 2.80MR10 52
- Fortinet
  - customer service 12
  - documentation 10
  - Knowledge Center 11

**I**

- icons in 2.80 18
- ips menu
  - anomaly 41
  - signature 40
- IPS, 2.80MR8 to 2.80MR10 62
- IPSec VPN, 2.80MR11 70

**L**

- LCD display changes 13
- log & report menu
  - log access 48
  - log config 46
- log config menu
  - log filter 47
  - log settings 46

**M**

- mark as clear spam action correction, 2.80MR11 68
- MIB fields, 2.80MR8 to 2.80MR10 54
- MTU settings for VLAN subinterfaces, 2.80MR11 65

**N**

- new features and changes
  - antivirus 41
  - firewall 39
  - ips 40
  - log & report 46
  - router 36
  - spam filter 43
  - system, admin 33
  - system, config 32
  - system, maintenance 34
  - system, network 31
  - system, sessions 31
  - system, status 31
  - system, virtual domain 35
  - user 39
  - vpn 39
  - web filter 42
- new features and changes for 2.80MR8 to 2.80MR10 50
- new features and changes to 2.80MR11 65
- Node Cards, 2.80MR11 65
- Node Cards, 2.80MR8 to 2.80MR10 57

**O**

- other issues for 2.80MR10 21
- other issues for 2.80MR11 19
- other issues for 2.80MR4 26
- other issues for 2.80MR5 25
- other issues for 2.80MR6 24
- other issues for 2.80MR7 24
- other issues for 2.80MR8 24
- other issues for 2.80MR9 23
- out of band management, 2.80MR8 to 2.80MR10 59

**P**

- perl expressions in 2.80 49
- phase 1 advanced settings, 2.80MR11 72
- phase 1 peer ID used in dynamic DNS config, 2.80MR8 to 2.80MR10 60
- phase 2 advanced options, 2.80MR11 72
- preventing public FortiGate interface from responding to ping requests, 2.80MR8 to 2.80MR10 50

**R**

- re-establishing
  - 2.50 connections 90
  - admin access settings 90
  - Internet connection 91
- replacement messages
  - converting to FortiOS 2.80 79
- restoring configuration
  - using the CLI 90

- using web-based manager 89
- router menu
  - key-chain 38
  - monitor 39
  - static 36

## S

- SMC 56
- SMC, 2.80MR11 65
- SMTP quarantine file name system generated 2.80MR11 67
- SMTP virus scanning only operates in splice mode, 2.80MR11 67
- spam filter email tagging for SMTP not supported, 2.80MR11 67
- spam filter menu
  - banned word 45
  - DNSBL and ORDBL 44
  - email address 45
  - fortiguard-antispam 44
  - IP address 44
  - MIME headers 45
- Spam Filter, 2.80MR11 74
- Spam filter, 2.80MR8 to 2.80MR10 64
- subnet specified for IP pool correction, 2.80MR11 68
- subordinate units block multicast and broadcast traffic in HA, 2.80MR8 to 2.80MR10 51
- subordinate units logging and SNMP in HA, 2.80MR8 to 2.80MR10 51
- subscription-based service name change, Fortinet 14
- support for FortiGate dialup clients, 2.80MR8 to 2.80MR10 61
- Switch Cards, 2.80MR11 65
- Switch Cards, 2.80MR8 to 2.80MR10 57
- system interface CLI forward\_domain, 2.80MR11 68
- system menu
  - admin 33
  - config 32
  - maintenance 34
  - network 31
  - sessions 31
  - status 31
  - virtual domain 35

## T

- technical support 12
- testing 2.80 before installing 76

## U

- unit information, 2.80MR8 to 2.80MR10 50
- updates to phase 1 peer options documentation, 2.80MR8 to 2.80MR10 59
- updating MAC forwarding tables when link failover occurs, HA 51

- upgrade notes
  - backup up config files 13
  - blade name change 14
  - CLI changes 17
  - Fortinet subscription-based service name change 14
  - icons in 2.80 18
  - LCD display changes 13
  - other 19
  - other issues for 2.80MR10 21
  - other issues for 2.80MR11 19
  - other issues for 2.80MR4 26
  - other issues for 2.80MR5 25
  - other issues for 2.80MR6 24
  - other issues for 2.80MR7 24
  - other issues for 2.80MR8 24
  - other issues for 2.80MR9 23
  - web-based manager changes 14, 17
- upgrading
  - 2.80 maintenance release from a system reboot using the CLI 84
  - 2.80 maintenance releases 81
  - 2.80 maintenance releases using the CLI 83
  - 2.80 maintenance releases using web-based manager 82
  - backing up configuration 75
  - config using CLI 76
  - testing firmware 76
  - using the CLI 78
  - using the web-based manager 78
  - verify testing firmware 77
- upgrading 2.80 firmware releases 81
- using perl expressions in FortiOS 2.80 49

## V

- verifying
  - downgrade to 2.50 88
  - test firmware 77
  - upgrade to 2.80 79
- VIP addresses for FortiClient dialup clients, 2.80MR8 to 2.80MR10 61
- VPN
  - 2.80MR8 to 2.80MR10 59
- vpn menu
  - IPSec 39
  - pptp 40
- VPN tunnel description update 2.80MR11 68

## W

- web filter menu
  - category block 43
  - script filter 43
  - URL block 42
- Web filter, 2.80MR8 to 2.80MR10 64
- web-based manager changes 14



**F**ORTINET™

[www.fortinet.com](http://www.fortinet.com)

**FORTINET™**

[www.fortinet.com](http://www.fortinet.com)