



What's New

FortiOS™ Handbook v3
for FortiOS 4.0 MR3



FortiOS™ Handbook What's New

v3

16 May 2012

01-437-117003-20120516

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Visit these links for more information and documentation for your Fortinet products:

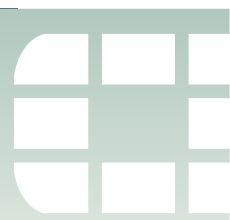
Fortinet Knowledge Base - <http://kb.fortinet.com>

Technical Documentation - <http://docs.fortinet.com>

Training Services - <http://campus.training.fortinet.com>

Technical Support - <http://support.fortinet.com>

You can report errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.



Contents

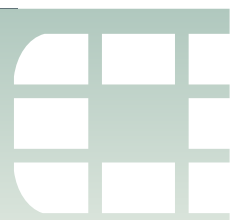
Introduction	9
How this guide is organized	9
Upgrading to FortiOS 4.0 MR3	11
General firmware upgrade steps	11
Backing up and restoring your FortiGate configuration file	12
Temporarily installing FortiOS 4.0 MR3	12
FortiOS 4.0 MR3 New Feature Highlights	15
Flow-based UTM Extensions	15
UTM Configuration and Inspection Enhancements	16
UTM profile and sensor configuration improvements	16
Archive inspection for antivirus profiles	17
Improved IPS default block rate	17
Web Filter profiles	17
Web Filtering Overrides	18
Application Control Sensors and filters	19
Geography-based filtering for firewall addresses	19
DLP document fingerprinting	20
Offloading UTM processing using Internet Content Adaptation Protocol (ICAP)	21
Profile Group	23
Modem interface Improvements	24
WiFi Extensions	24
WiFi controller redesign	25
Captive portal enhancements	25
Rogue AP detection and reporting	26
Custom AP profiles	26
Distributed ARRP (Automatic Radio Resource Provisioning)	26
WiFi monitor	27
New WiFi commands	27
Strong Authentication Enhancements	28
FortiToken support	28
Two-factor authentication	29
Enabling two-factor authentication for administrators	30
Multiple authentication group enforcement	31
Dynamic Profiles	31
Hard-timeout enhancement	32
PKI certificate authentication enhancement	32
NTLM authentication enhancements	33

New PCI Compliance Features	33
Feature Improvements to extend IPv6 support	35
Top Session dashboard widget IPv6 support	35
OSPFv3 NSSA extension	35
Explicit proxy and web caching improvements	36
Explicit FTP proxy	36
Explicit Web Proxy Forwarding Servers (proxy chaining)	37
Authentication cookie for session-based authentication of explicit web proxy sessions	38
Form-based user authentication for explicit web proxy	38
Web caching in security policies	38
Logging and reporting enhancements	41
FortiGuard Analysis and Management Service (FAMS)	41
Adding FortiGate units to FAMS	43
Sending log messages to FAMS	43
Viewing FAMS reports from a FortiGate unit	44
Logging performance optimization for FortiOS 4.0 MR3 patch 7	44
FortiAnalyzer real time logging no longer requires disk logging	44
SQL database moved from the log disk to system memory for some models	44
Disabling extended traffic logging	44
Reducing SQL logging database size	45
Disable SQL logging filters on the local disk	45
Disable SQL logging on AMC disk models (ASMS08)	45
The FortiGate UTM Weekly Activity Report	46
Viewing the current and historical reports	48
Creating custom reports from the CLI	49
Log Access Improvements	49
Viewing log messages	49
Filtering log messages	50
Downloading log messages	50
New Unified UTM Log Access	50
SQL logging enabled by default	51
Sending DLP archives to multiple FortiAnalyzer units	52
Remote logging configuration enhancements	52
Log and Report Monitoring	52
Logging Monitor	53
Log Message Enhancements	53
Event logs	53
Event-system	54
Traffic logs	54
Other-traffic logs	54
Chat message log support for MSNP21	54

SSL connection encryption level option over OFTP	54
Uploading logs to a FTP server in text format	55
Example for uploading logs to a FTP server in text format	55
Deleting all local logs, archives and user-configured report templates	56
FortiOS 4.0 MR3 Usability improvements	57
High-level web-based manager menu changes	57
New FortiGate Setup Wizard	58
FortiExplorer enhancements	58
Dashboard Widgets	58
Traffic History	59
System Resources	59
Network Protocol Usage	60
Chart display improvements	61
Monitoring Improvements	61
DHCP Monitor	61
Modem Monitor	62
Session Monitor	62
Policy Monitor	62
Load Balance Monitor	62
Traffic Shaper Monitor	62
AV Monitor	63
Intrusion Monitor	63
Web Monitor	63
Email Monitor.	63
Archive & Data Leak Monitor.	63
Application Monitor	64
IPsec Monitor	64
SSL-VPN Monitor	64
Web Cache Monitor	64
WAN optimization Peer Monitor	64
WAN optimization web cache monitor.	64
Filtering web-based manager lists	65
Reference count column (object usage visibility).	66
Configuration object tagging and coloring	68
Adding tags to configuration objects	69
Example of how to find a security policy using Tag Management.	69
Adding tags to predefined signatures and applications	70
Security configuration object icons	71
Access to online help.	71
Backing up and restoring configuration files per-VDOM.	71

More New Features	73
New features for FortiOS 4.0 MR3 Patch 7	74
New features for FortiOS 4.0 MR3 Patch 6	74
New features for FortiOS 4.0 MR3 Patch 5	74
New features for FortiOS 4.0 MR3 Patch 4	75
New features for FortiOS 4.0 MR3 Patch 3	75
New features for FortiOS 4.0 MR3 Patch 2	75
New features for FortiOS 4.0 MR3 Patch 1	76
Login grace timer for SSH connections	78
FortiManager automatic authorization	78
Dynamic DNS commands	78
New diagnose commands	78
Real-time session, traffic shaper bandwidth and CP6 statistics.	78
diag sys session filter proto-state	79
diag log-stats show	79
New get commands	79
IPsec get commands.	79
Traffic shaper and per-IP shaper.	80
Management checksum configuration information for FortiManager	80
MTU configuration support on non-IPsec tunnel interfaces	81
Customizing maximum number of invalid firewall authentication attempts	81
Controlling the connection between a FortiManager unit and a FortiGate unit	81
Bringing up or down IPsec tunnels.	81
Configuring active CPUs	82
Formatting multiple disk partitions	82
Transparent mode port pairs	83
DNS server changes	83
DHCP Server changes	84
DHCP IP Reservation	84
Installing firmware on a partition without a reboot	84
Example of installing a firmware on a partition without rebooting	85
SNMP enhancements	86
WAN optimization, Web Cache and Explicit proxy MIBs	86
SNMPv3	86

Replacement message changes	86
Archive replacement messages and FTP proxy replacement message	87
Successful firewall authentication replacement message	87
Web filtering disclaimer replacement message	87
Video chat block replacement message	87
Replacement message images	87
VDOM and global privileges for access profiles	88
Example of incorporating the new access profile to existing administrator accounts.	88
HA dynamic weighted load balancing	89
Configuring weighted-round-robin weights	89
Dynamic weighted load balancing	91
Example weighted load balancing configuration	92
VRRP virtual MAC address support	93
FGCP HA subsecond failover	94
Static Route enhancements	94
Monitoring ISIS from the Routing Monitor page	95
Security Policy and Firewall Object Enhancements	95
Source IP addresses for FortiGate-originating traffic	95
Example of using the source IP address feature to track logs at a syslog server	95
Local-in security policies	96
Protocol Options	96
FTPS support	96
Virtual IP source address filter support.	97
Virtual IP port forwarding enhancements.	97
Load balancing HTTP host connections	97
Web Proxy Service and Web Proxy Service Group	97
SSL renegotiation for SSL offloading provides allow/deny client renegotiation	98
SSL VPN Port forwarding support	98
IKE negotiation	98
SHA-384 and SHA-512 support for IKE	99
FortiOS Carrier URL extraction feature.	99
Appendix	101
Index	107



Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This chapter of the FortiOS Handbook describes the new features and changes to existing features that are available in FortiOS 4.0 MR3.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

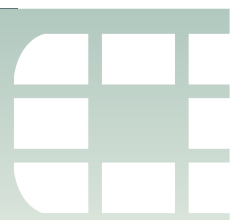
[Upgrading to FortiOS 4.0 MR3](#) provides information about upgrading to the new release.

[FortiOS 4.0 MR3 New Feature Highlights](#) describes the key new features available in FortiOS 4.0 MR3.

[Logging and reporting enhancements](#) describes new logging and reporting features.

[FortiOS 4.0 MR3 Usability improvements](#) describes FortiOS 4.0 MR3 usability enhancements and changes.

[More New Features](#) describes other general new FortiOS 4.0 MR3 features and lists what's new in FortiOS 4.0 MR3 patches 1 to 5.



Upgrading to FortiOS 4.0 MR3

This section explains how to properly upgrade to FortiOS 4.0 MR3. The following topics are included in this section:

- [General firmware upgrade steps](#)
- [Backing up and restoring your FortiGate configuration file](#)
- [Temporarily installing FortiOS 4.0 MR3](#)

General firmware upgrade steps

Regardless of whether you are installing the 4.0 MR3, patch release or GA firmware, you should use the following general procedure as a guideline for installing the firmware image. Upgrade the firmware during a low-traffic time period to avoid disrupting your network.

For more information about upgrading to FortiOS 4.0 MR3 see the FortiOS 4.0 MR3 Release Notes.

General procedure for upgrading current firmware - web-based manager

- 1 Verify what firmware image you need to upgrade to from the current firmware image that is running on the unit.
- 2 Download the new firmware image.
- 3 Back up your current configuration file.
- 4 Log into the web-based manager and go to *System > Dashboard > Status* and in the System Information Widget select *Update* beside the *Firmware Version*.
- 5 Select the firmware image file to install.
- 6 Clear your browser's cache after the installation process is finished.
After a few minutes you can log back into the web-based manager.
- 7 Manually update antivirus and intrusion protection definitions and engines to the current version.

Go to *System > Config > FortiGuard > Antivirus and IPS Options* and select *Update Now*.

The signatures included with a firmware image upgrade may be older than ones currently available from FortiGuard.

Backing up and restoring your FortiGate configuration file



Always back up your FortiGate configuration before upgrading or downgrading firmware, or resetting configuration to factory defaults. Then if required you can restore the configuration by uploading the backed up configuration file to your FortiGate unit.

Before installing any firmware image, you should back up the current FortiGate configuration file. This ensures that you have a current configuration file if the upgrade is not successful. You are also ensuring that all configuration settings are available if there are some that are not carried forward.

To back up your configuration file - web-based manager

- 1 Log into the web-based manager and go to *System > Dashboard > Status* and in the System Information Widget select *Backup* beside *System Configuration*.
- 2 Select where to save configuration file.
- 3 If you want to encrypt your configuration file to save VPN certificates, select *Encrypt configuration file* and enter and confirm a password. An encrypted configuration file can only be opened by uploading it to the same FortiGate unit and entering this password.
- 4 Select *Backup* and save the configuration file.

To restore your configuration file - web-based manager

You may need to restore your configuration file if you have experienced problems during a firmware upgrade.

- 1 Log into the web-based manager and go to *System > Dashboard > Status* and in the System Information Widget select *Restore* beside *System Configuration*.
- 2 Select to configuration file to restore.
- 3 If the configuration file is encrypted, enter the password.
- 4 Select *Restore* to restore the configuration to the one of the saved the configuration file.

The FortiGate unit uploads and installs the configuration.

- 5 Clear your browser's cache after the installation process is finished.
After a few minutes you can log back into the web-based manager.

Temporarily installing FortiOS 4.0 MR3

The following procedure describes how install temporarily install a firmware image to the system memory. When you reboot the FortiGate unit it will restart running the current firmware.

The procedure describes how to reboot the FortiGate unit and download firmware from a TFTP server and select the `Run image without saving` option to temporarily store the firmware image in memory without upgrading the firmware image stored on the FortiGate bootup device.

This procedure provides a way to become familiar with new FortiOS 4.0 MR3 new features and changes before committing to a full upgrade to the new version.

To temporarily install a new firmware image

- 1 Copy the new firmware image file to the root directory of a TFTP server.

- 2 Set up a console connection to the FortiGate unit CLI.
- 3 Make sure the FortiGate unit can connect to the TFTP server using the `execute ping` command.
- 4 Restart the FortiGate unit. For example, enter the following command:
`execute reboot`
- 5 As the FortiGate unit reboots, press any key to interrupt the system startup when the following message appears:
Press any key to display configuration menu ...

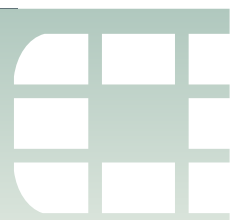


You have only three seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

- 6 If you successfully interrupt the startup process, a message similar to the following appears:

```
[G]: Get firmware image from TFTP server
[F]: Format boot device
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default firmware
[H]: Display this list of options.
```

Enter G, F, Q, or H:
- 7 Type G to get the new firmware image from the TFTP server.
The following message appears:
Enter TFTP server address [192.168.1.168]:
- 8 Type the address of the TFTP server and press Enter.
The following message appears:
Enter Local Address [192.168.1.168]:
- 9 Type an IP address of the FortiGate unit 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]:
- 10 Enter the firmware image file name and press Enter.
The TFTP server uploads the firmware image file to the FortiGate unit and the following appears:
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
- 11 Type R.
The firmware image is installed to system memory and the FortiGate unit starts running the new firmware image, but with its current configuration.
- 12 When you are done, reboot the FortiGate unit and it will resume using the previous firmware image.



FortiOS 4.0 MR3 New Feature Highlights

This section describes the key new features available in FortiOS 4.0 MR3. In addition to the highlights described in this section see “[Logging and reporting enhancements](#)” on [page 41](#) for information about the new logging features in FortiOS 4.0 MR3 and “[FortiOS 4.0 MR3 Usability improvements](#)” on [page 57](#) for complete information about all of the usability improvements in FortiOS 4.0 MR3.

- [Flow-based UTM Extensions](#)
- [UTM Configuration and Inspection Enhancements](#)
- [Modem interface Improvements](#)
- [WiFi Extensions](#)
- [Strong Authentication Enhancements](#)
- [New PCI Compliance Features](#)
- [Feature Improvements to extend IPv6 support](#)
- [Explicit proxy and web caching improvements](#)

Flow-based UTM Extensions

Flow-based inspection can result in major performance improvements to UTM inspection. First introduced to improve antivirus performance in FortiOS 4.0 MR2, in MR3 flow-based inspection has been extended to web filtering and data leak prevention (DLP) and also includes the ability to virus scan compressed files.

This flow-based scanning performance improvements come from reduced memory requirements, high concurrent session count, high session start rates and low latency. In addition flow-based scanning is not affected by a maximum file size.

The trade-off for these advantages is that flow-based scanning may not be as accurate or comprehensive as proxy-based scanning although Fortinet is continuing to improve the accuracy and depth of coverage provided by flow-based UTM features.

Flow-based web filtering

Flow-based web filtering is a non-proxy solution which provides high concurrent session, high session rate, and low-latency web-filtering service. You can enable flow-based web filtering within a web filter profile.

You can enable flow-based web filtering in any Web Filter Profile by setting the *Inspection Mode* to *Flow-based*. Flow-based web filtering can be enabled in some web filtering profiles and not others, allowing you to apply flow-based web filtering to some traffic and proxy-based web filtering to other traffic.

Flow-based Data Leak Prevention (DLP)

Flow-based DLP is a non-proxy solution which provides high concurrent session, high session rate, and low-latency DLP services. You can enable flow-based DLP within a DLP sensor.

You can enable flow-based DLP in any DLP Sensor by setting the *Inspection Method* to *Flow-based Detection*. Flow-based DLP can be enabled in some DLP sensors and not others, allowing you to apply flow-based DLP to some traffic and proxy-based DLP to other traffic.

UTM Configuration and Inspection Enhancements

FortiOS 4.0 MR3 includes the following improvements to UTM functionality.

UTM profile and sensor configuration improvements

All UTM features including Antivirus, intrusion protection, web filtering, email filtering, data leak prevention, application control, VoIP and ICAP include one or more default profiles or sensors. In many cases you can add the default profile or sensor to a security policy to apply basic functionality for that UTM feature. You can also modify the default profiles and sensors to meet your requirements and create new profiles and sensors.

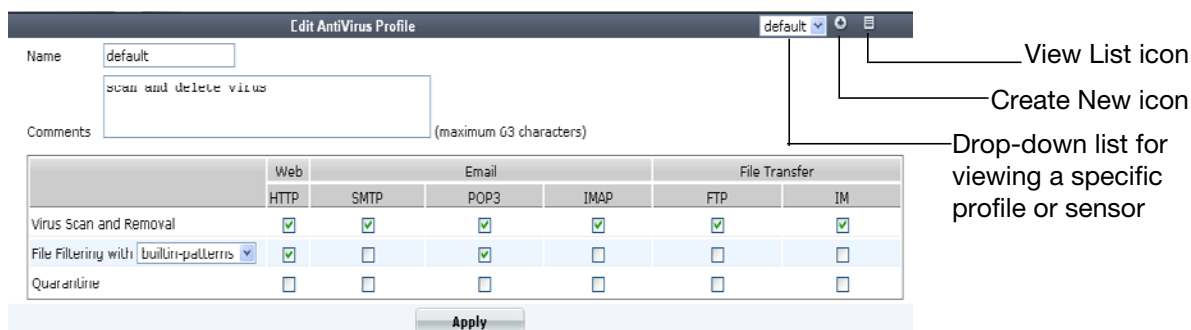
Within the Configuration Settings page for all UTM features you can do the following:

- view and edit the default profile or sensor
- view the current settings of a profile or sensor
- create or remove a new profile or sensor
- view a list of profiles or sensors that you created

In the upper-right corner of the Configuration Settings page there is a drop-down list, *Create New* icon and *View List* icon. These are shown in Figure 1. You can use them in the following ways:

- Create a new profile or sensor by selecting *Create New*.
- View a specific profile or sensor by selecting it from the drop-down list.
- View the profiles or sensors that you have created by selecting *View List*.
- Remove the current profile or sensor that you are viewing by selecting *Delete*.

Figure 1: Example antivirus profile page



The actual configuration operations for all UTM profiles and sensors has also been modified to make configuration of sensors and profiles faster and more effective.

Archive inspection for antivirus profiles

Within antivirus profiles, you have more control about how the FortiGate unit handles file archives (for example .zip files). These options have been added because some archives cannot be virus scanned (for example, encrypted archives).

From the CLI you can select options to block all encrypted archives, block corrupted archives, block multipart archives, and write log messages whenever an archive file is received that cannot be virus scanned.

The following is an example.

```
config antivirus profile
edit av_1
config http
set options block-encrypted-archive block-corrupted-
archive block-multipart-archives log-unhandled-archive
end
```

Improved IPS default block rate

The IPS default block rate was improved so that the critical level, high level and medium levels are now higher. The critical level now has an 80 percent default block rate or higher; high level has 70 percent or higher; and the medium level has 50 percent rate or higher.

IPS signature rate count threshold

The IPS signature threshold has been enhanced to allow you to configure a signature that will not be triggered until a rate count threshold is met. This provides a better, more controlled recording of attack activity. For example, multiple login-failed events are detected in a short period of time, and an alert is raised.

This enhancement is enabled from the CLI. Once you enter a value for the rate count you can configure the rate limit mode optionally the packet fields to track. The command syntax is:

```
config ips sensor
edit <sensor_name>
config override
edit 0
set rate-count <integer>
set rate-duration <integer_seconds>
set rate-mode {continuous | periodical}
set rate-track {dest-ip | dhcp-client-mac | dns-domain |
none | src-ip}
end
```

IPS Predefined signature viewer

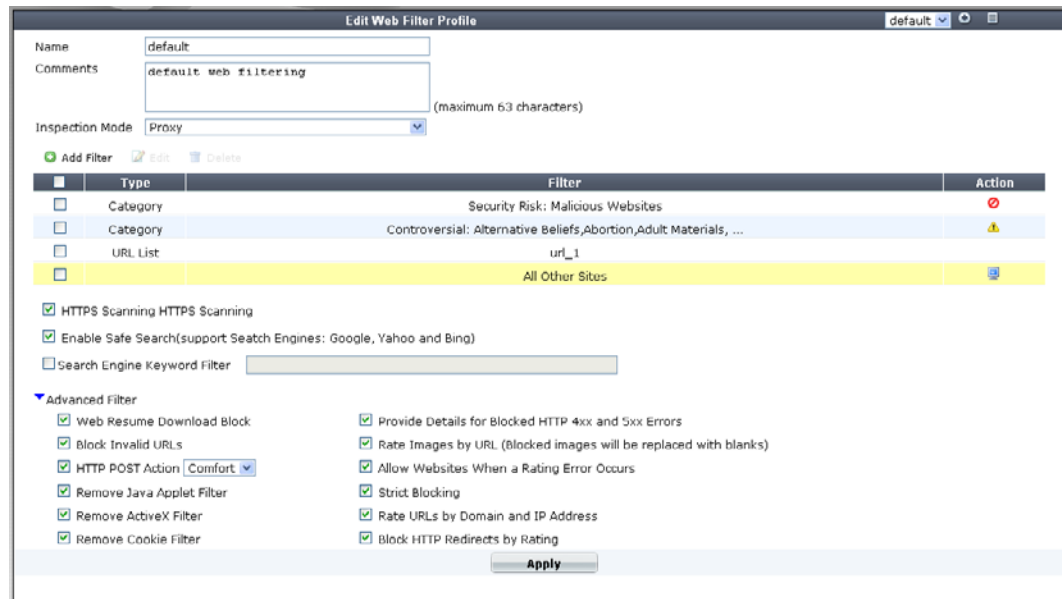
When you are viewing predefined signatures in *UTM Profiles > Intrusion Protection > Predefined*, you can more easily view information about each signature using the IPS Signatures Viewer.

Web Filter profiles

In *UTM Profiles > Web Filter > Profiles*, the Web Filter Profile Configuration Settings page contains a complete redesign of what was previously there. Previously, there was FortiGuard Web Filtering and FortiGuard Web Filtering Overrides; these are now in the CLI. Filters can be added to the profile. A filter is a category or banned word.

The Web Filtering feature contains the following new features and changes to existing features. The Web Filter menu no longer contains the submenu Web Content Filter; however, these settings are still available in the CLI.

Figure 2: The default configuration settings on the Edit Web Filter Profile page



Previous web filter profiles are carried forward and those settings are merged into the new redesign. If you want to view the previous settings in FortiOS 4.0 MR3, use the `show webfilter profile <name>` command to view the entire previous settings.

Depending on what settings you need to configure within the web filter profile, you may need to have access to both the CLI and web-based manager. The FortiGuard Web Filtering, FortiGuard Web Filtering Overrides and web content filtering are now configured in the CLI.

In a web filter profile, you can also include keywords that may appear in a search engine that a user enters in a search engine. These keywords are logged in the web filter log. The keywords are entered, separated with a comma, in the *Search Engine Keyword Filter* field.

Web Filtering Overrides

Web filtering overrides are now simplified and are profile-based. Profile-based overrides are web filter profiles that contain only overrides, and these overrides allow a rule to be created that changes the web-filter profile that applies to a user. The override feature is extended to apply to all features within the web-filter profile, and an override link appears in all related blocked pages where the user can override the block and continue on.

When you want to create a web filtering override, create a new web filter profile that is specifically for overrides. These configuration settings are available only in the CLI. These settings in the new override profile are configured by the administrator, and the administrator has complete control over the changes for the user.

The command syntax for configuring a new profile-based web filter override is as follows:

```
config webfilter {override | override-user}
  edit <id_number>
    set expires <yyyy/mm/dd hh:mm:ss>
    set initiator admin
```

```
set status {enable | disable}
set old-profile <old_profile_name>
set new-profile <new_profile_name>
set scope {ip | ip6 | user |user-group}
set user <user_name>
set user-group <user_group_name>
end
```



For the option `initiator`, its value is always `admin`.

In the above command syntax, you see the commands `old-profile` and `new-profile` and its these commands that control how the override rule is applied. For example, if a user is browsing using a session that contains an old web filter profile applied, then the new-profile is used instead. If a user browses using a session that has a profile other an old profile, their profile will not be changed to a new profile. A user may be able to create a new override rule if the configuration permits it; however, only one override rule is allowed per user/profile pair.

With a web filter profile-based override, you can modify the URL filter list or add local ratings to deal with the extraction of offsite URLs. However, the function of this new override may change a user's FortiGuard categories, URL-filter list and so on.

When upgrading, existing web-filter profiles are carried forward but will not work until the administrator modifies them to the new settings. Any existing rules, both user and administrative, are not carried forward because there is no way to change the old override type to profiles for each rule without running out of profiles. This concerns only administrative overrides.

Application Control Sensors and filters

Application Sensors are similar to IPS or DoS sensors and replace the application control lists available in FortiOS 4.0 MR2.

An Application sensor contains application filters which you can configure to select individual applications to control or you can use categories, vendor names, behavior types, technology types, protocols, and tags to select groups of related applications. Application filters allow you to monitor, block, and reset sessions for single applications or groups of applications.

Application filters also allow you to apply shared traffic shaping to applications in the filter. You can apply forward and reverse traffic shaping and if the traffic shaper includes DSCP (or DiffServ) settings, these are also applied to applications specified in the filter. You can also set the session TTL for different applications and enable packet logging for applications.

Fortinet is constantly adding more applications to application control. Recent additions include the ability to individually monitor and block many Facebook applications.

Geography-based filtering for firewall addresses

Geography-based filtering for firewall addresses allows you to create a firewall address consisting of the name of a country. You can then add this address to a security policy to match traffic from any IP address assigned to that country. The list of countries and IP addresses that the FortiGate unit uses to identify the country of origin of an address is based on historical data compiled from the FortiGuard network.

For example, to configure a security policy to allow connections to multiple branch offices in Brazil (headquarters are in United States); the source address in this particular policy is *Any*, destination address is Brazil (geographic firewall address) and the *Action* is *Allow*.

To add a geography-based firewall address from the web-based manager, go to *Firewall Objects > Address*, select *Create New*, set *Type* to *Geography* and select a country name.

Use the following command to add a geography-based firewall address for Brazil:

```
config firewall address
  edit <addr_name>
    set type geography
    set country BR
  end
```

In the command you set the `country` to the two-letter abbreviation for the country name. In the example, `BR` is the abbreviation for Brazil.

You can use the following command to view information about geography-based addressing. The command does not display information about the entire address database, but displays country and address information for the countries that have been added to firewall addresses.

```
diagnose firewall ipgeo {country-list | ip-list | ip2country}
```

Where:

`country-list` lists all of the countries that have been added to a firewall address.

`ip-list` lists the IP addresses of a specified country or all of the countries added to firewall addresses.

`ip2country` displays the country of origin for a specified IP address. The address must be assigned to one of the countries that has been added to a firewall address.

For example, use the following command to view the countries that have been added to a firewall address. The example command output shows that a firewall address has been added for Brazil.

```
diagnose firewall ipgeo country-list
Total countries loaded:1

BR
```

DLP document fingerprinting

DLP document fingerprinting is a new feature that allows you to better protect your network from the loss of specific documents. Document fingerprinting, in this sense, is a method of identifying a document. This method breaks up files into chunks, taking a checksum of those chunks and using that checksum as the fingerprint. The fingerprint is then applied to a DLP filter rule within a DLP sensor which is then used during the scanning process of DLP activity.

DLP document fingerprinting is configured in *UTM Profiles > Data Leak Prevention > Document Fingerprinting* and then a DLP filter rule is applied within a DLP Sensor in *UTM Profiles > Data Leak Prevention > Sensor* to instruct the FortiGate unit to look for document fingerprints when scanning DLP activity on a security policy. A percentage parameter set in the DLP sensor is used when the unit is trying to match the file chunks.

For example, you transfer a file that is on the server (or uploaded), it will match 100 percent; a truncated file on the server will be matched 100 percent except for possibly the first or last chunks that may have a different checksum because the boundaries are different. The same is true for a file that is partially copied into another file; if that part is large enough, it will match but at a low percentage.

All documents in the source, as well as the ones you uploaded individually, are pre-scanned. This means that the task of breaking the files into checksums occurs soon after creating them and are all put into the database on the FortiGate unit.

There is an option to upload archived files and have those archived files fingerprinted as well, however, this is for only individual files that are configured in *Manual Document Fingerprints* on the DLP Fingerprint page.



DLP document fingerprinting is available only on FortiGate models with internal hard drives or flash drive storage.

Offloading UTM processing using Internet Content Adaptation Protocol (ICAP)

The Internet Content Adaptation Protocol (ICAP) is supported in this release. ICAP is a light-weight response/request protocol that allows the FortiGate unit to offload HTTP and HTTPS traffic to external servers for different kinds of processing. ICAP is often used for offloading UTM features such as virus scanning, DLP and web filtering but has many other applications.



ICAP does not appear by default in the web-based manager. You must enable it in *System > Admin > Settings* to display ICAP in the web-based manager.

If you enable ICAP in a security policy, HTTP traffic intercepted by the policy is transferred to an ICAP server in the ICAP profile added to the policy. Responses from the ICAP server are returned to the FortiGate unit which forwards them to an HTTP client or server.

You can offload HTTP responses or HTTP requests (or both) to the same or different ICAP servers.

If the FortiGate unit supports HTTPS inspection, HTTPS traffic intercepted by a policy that includes an ICAP profile is also offloaded to the ICAP server in the same way as HTTP traffic.

Example ICAP sequence for an ICAP server performing web URL filtering on HTTP requests

- 1 A user opens a web browser and sends an HTTP request to connect to a web server.
- 2 The FortiGate unit intercepts the HTTP request and forwards it to an ICAP server.
- 3 The ICAP server receives the request and determines if the request is for URL that should be blocked or allowed.
 - If the URL should be blocked the ICAP server sends a response to the FortiGate unit. The FortiGate unit returns this response to the user's web browser. This response could be a message informing the user that their request was blocked.
 - If the URL should be allowed the ICAP server sends a request to the FortiGate unit. The FortiGate unit forwards the request to the web server that the user originally attempted to connect to.

When configuring ICAP on the FortiGate unit, you must configure an ICAP profile that contains the ICAP server information; this profile is then applied to a security policy.

Example of adding ICAP to a security policy

The following is an example of configuring the ICAP feature on the FortiGate unit and applying an ICAP profile to an existing security policy.

1 Log in to the CLI.

2 Enter the following to configure the ICAP server:

```
config icap server
  edit icap_server
    set ip-address 172.16.122.151
    set ip-version 4
    set max-connections 25
    set port 453
  end
```

3 Enter the following to configure the ICAP profile to then apply to a security policy:

```
config icap profile
  edit icap_profile_1
    set request enable
    set request-failure error
    set request-path 1220
    set request-server icap_server
    set response enable
    set response-failure error
    set response-path 1225
    set response-server 172.16.122.151
    set streaming-content-bypass enable
  end
```

4 In the `config firewall policy` command, apply the ICAP profile to policy 1:

```
config firewall policy
  edit 1
    set icap-profile icap_profile_1
  end
```

Troubleshooting ICAP

You can use the following diagnose commands when troubleshooting ICAP.

```
diag system icap server list <name>
```

Displays a list of all servers or specified servers.

```
diag system icap profile list <name>
```

Displays information concerning total sent and responses, last connection attempts and host-bypass count.

Profile Group

The Profile Group feature is now included in the web-based manager of some models. This feature was previously only found in the CLI. Profile groups are groups of UTM profiles and sensors, which includes protocol options, and are often applied to security policies. By configuring a group of profiles and sensors, you can easily apply them to a security policy at once, instead of enabling them one at a time.

In *UTM Profiles > Profile Group > Profile Group*, you can create profile groups and view the selected profiles from within the group, either when creating a new group or editing an existing one. You can view the profile or sensor that you are including in the group by selecting the *View* icon. You can also create a new profile or sensor from within the page by selecting the *Create New* icon (the plus sign icon).



In this release, profile groups cannot be applied to security policies within the web-based manager, only in the CLI.

Modem interface Improvements

The Modem interface feature has been updated to include settings for configuring 3G or 4G wireless modems, as well as other modems. A list of supported modems is available from FortiGuard and can be updated to include recently supported modems.

When you first go to *System > Network > Modem*, the configuration settings within the page have changed, and now there is a *General Settings* section and *External Modem* section. The *General Settings* section is for configuring the primary modem, for example an external modem. You can still configure the modem to be *Standalone* or *Redundant* from this page, as well the type of *Dial Mode*.

The *External Modem* section of the page allows you to configure the external modem or USB modem. When you select *Configure Modem*, you are automatically redirected to the Modem Configuration Settings page. This page displays the supported modems under the *Supported* section, and the *Custom* section displays the external modems that you have configured. By selecting *Update Now*, you can easily update the list of supported modems from FortiGuard.

3G/4G modem list available from FortiGuard

You can now access a list from FortiGuard that contains all support 3G and 4G modems. The list is available without a subscription. By default, a list of supported modems is available on the FortiGate unit; however, you can update this list at any time from FortiGuard.

The list is available within the Modem page, on the Modem Selection page. This page appears when you select *Configure Custom Modem*. You can either update this page or choose a modem from the list.

WiFi Extensions

FortiOS 4.0 MR3 includes many improvements and changes to the WiFi controller feature (formerly the wireless controller feature). Among the highlights are automatic AP provisioning (channel, power, etc.) using distributed ARRP, Rogue AP “on wire” detection, Rogue AP Suppression, Unified FortiWifi and FortiAP management, support for new FortiAP models, and the addition of the WiFi controller feature to FortiWiFi units.

WiFi controller redesign

On the web-based manager the former wireless controller has been renamed *WiFi Controller* and menus and submenus have been redesigned as follows:

- WiFi Network
 - SSID
 - Rogue AP Settings
- Managed Access Points
 - Managed FortiAP
 - Custom AP Profile
- Monitor
 - Client Monitor
 - Rogue AP Monitor

Within the WiFi Network menu, instead of configuring a virtual access point, you configure an SSID. The SSID can easily be configured to be up or down, using the *Administrative Status* option within the SSID.

When configuring an SSID from the web-based manager you can choose from any of the following consolidated security options:

SSID security option	Descriptions
WPA/WPA2-Personal	Supports both WPA and WPA2 for personal use. Select this option and add a 8 to 63 character preshared key.
WPA/WPA2-Enterprise	Supports both WPA and WPA2 for enterprises. Select this option and select a RADIUS server or authentication group to use to authenticate connections to the SSID.
Captive Portal	Supports captive portal authentication. Select this option and select user groups that can authenticate with the captive portal. You can also configure the appearance of the captive portal page.

Configure an SSID from the CLI using the `config wireless-controller vap` command. From the CLI the following additional security options are available:

- open
- wep128
- wep64
- wpa-only-enterprise
- wpa-only-personal
- wpa2-only-enterprise
- wpa2-only-personal

Captive portal enhancements

The captive portal security option was previously available; however, in this release it has been enhanced and given additional replacement messages so that you can have specific pages for specific actions, such as when a failed login attempt or a declined disclaimer. The captive portal security is now more streamlined and is applied within an SSID, instead of previously being applied within a security policy.

Rogue AP detection and reporting

The PCI DSS regulatory compliance requires quarterly site surveys for unauthorized wireless access points on their networks to prevent data leakage, as well as assurance that trusted access points are running the latest WPA or WPA2 enterprise encryption. In this release, you can now easily gather this information and view it on the FortiGate unit.

From the WiFi Controller menu, you can configure the FortiGate unit to gather information on rogue APs, monitor them, and then take the information gathered from logs and generate a report.

The Rogue AP Settings submenu enables detecting rogue wireless access points. The option, *Enable On-Wire Rogue AP Detection Technique*, is a special detection technique that allows the FortiGate unit to help identify rogue APs that may be performing a bridging function, routing or NAT.

Rogue AP Suppression

Rogue AP suppression is now supported on the FortiWiFi and FortiAP units. This feature is available only when there is at least one radio signal dedicated to Rogue AP detection. On a FortiWiFi unit, this feature is available only when in dedicated detection mode. Rogue AP suppression is also not available for background Rogue AP scans.

On-wire Rogue AP detection

The on-wire scan feature allows you to detect if a rogue AP is connected to a wired network. A rogue AP poses a higher security risk if that rogue AP is an unmanaged AP and connected to an organization or company's wireless network. A rogue AP is an AP that is not managed by the controller.

To enable on-wire scan rogue AP detection go to *WiFi Controller > Wireless Network > Rogue AP Settings* and select *Enable On-Wire Rogue AP Detection Technique*.

Custom AP profiles

Previously, there were access point (AP) profiles that you could configure from within the WiFi Controller menu. These profiles are still available, however, to view them in the web-based manager you must enable the feature using the following command.

```
config system global
  set gui-ap-profile enable
end
```

Under Managed Access Points, the previous AP Profile menu has been replaced with the Custom AP Profile menu that contains a selection of default AP profiles. These default profiles have been designed to be a good starting point for many wireless network applications using FortiWiFi or FortiAP units. You can customize the default profiles for your needs and create new profiles.

Distributed ARRP (Automatic Radio Resource Provisioning)

For FortiAP units, each unit needs to autonomously and periodically determine the best channel that is best suited for communication. The distributed ARRP feature allows FortiAP units to select their channel so that they do not interfere with each other in a larger square footage network scenario.

The distributed ARRP behaves in the following way:

- Each FortiAP unit independently scans the available channels, measuring interface and channel utilization, and then selecting the channel with the least interface and then lowest utilization for communication.

- The FortiAP unit periodically performs this scan in the background to determine if any conditions have changed. This periodical scan is every ten minutes (by default).
- If any conditions have changed, the FortiAP unit signals all clients to move to a newly selected channel.

Log messages are recorded to reflect when the channel was changed by the FortiAP unit, and debug logs are also recorded to reflect the decision of the distributed ARRP algorithm for all runs. The ARRP algorithm is automatically on by default if multiple channels are selected in the web-based manager. If a single channel is selected, the ARRP algorithm becomes benign.

WiFi monitor

The WiFi Monitor menu is a new WiFi Controller feature in this release. It merges the previous monitoring menus into the new Monitor menu. There are two submenus, Client Monitor and Rogue AP Monitor.

The Client Monitor submenu allows you to view information about wireless clients of your managed access points. On the Client Monitor page, several columns have changed, as well as a new column added, called Auth. The following columns are no longer available on the page:

- Bandwidth Rx
- Bandwidth Tx
- Idle Time

Previously, the Client Monitor was available in *WiFi Controller > Wireless Client > Wireless Client*.

The Rogue AP Monitor allows you to view information about access points that may be rogue APs. Several columns have been removed. There are two new columns, Manufacturer and Security Mode. From the monitor you can also mark and suppress APs.

New WiFi commands

The following are new commands regarding WiFi server certificates and user group authentication for WiFi.

Certificate commands:

```
config system global
  set wifi-certificate <cert_name>
  set wifi-ca-certificate <ca_cert_name>
end
```

Authentication user group commands:

```
config system interface
  edit <wlan>
    set wifi-auth usergroup <user_name>
  end
```

The `wifi-auth usergroup` command is available only if WPA-Enterprise or WPA2-Enterprise option is selected as the security mode.

The authentication user group commands also apply to WiFi Controller.

Strong Authentication Enhancements

FortiOS 4.0 MR3 new strong authentication features include support for the FortiToken two-factor (2-factor) authentication solution as well as two-factor authentication using Email or SMS. Additional new strong authentication features include improved multiple user group support, dynamic profiles, and PKI authentication enhancements.

FortiToken support

The FortiToken-200 device provides time-based, one-time passwords (OTP) that are based on the Open Authentication (OATH) standard. Using FortiToken allows organizations to deploy a two-factor authentication solution that reduces the risk of compromise created by alternative single-factor authentication systems relying on, for example, static passwords. The FortiToken enables administrators with the need for two-factor authentication to offer enhanced security for both remote and on-premise users. The FortiToken-200 is a part of Fortinet's broad multi-factor authentication product strategy; it ensures that only authorized individuals access your organization's sensitive information; enabling business, protecting your data, lowering IT costs, and boosting user productivity.

The FortiToken-200 provides a secure one-time password (OTP) that is entered along with regular login credentials whenever authentication is required.

Each FortiToken device contains a serial number (located on the back of the device), a six-digit LCD display, and a small button. The serial number is used to activate the hardware token generator. When you press the small button, the LCD displays a six-digit token password code that is used in two-factor authentication. Two-factor authentication is authentication that requires an additional password or code that a user must enter to successfully authenticate in addition to their own user name and password.

The FortiToken device must be activated and synchronized with the FortiGate unit before it can be used for authentication purposes.

The FortiToken behaves as follows:

- FortiToken's serial number is added in the list in *User > FortiToken > FortiToken*. This serial number is a number containing 16 case-sensitive characters which is located on the back of the device. The serial number is used only in this way.
- The FortiToken is activated by selecting *Activate* on the FortiToken page. During the activation process the serial number is encrypted and sent to FortiGuard where it is verified as a valid FortiToken, and then activates the FortiToken on the FortiGate unit. If you have a file containing the seed used to generate a token password code, you can import that file to the FortiGate unit from *User > FortiToken > FortiToken*.
- Synchronize the FortiToken by selecting *Synchronize* on the FortiToken page. This synchronizes the FortiToken's system time with the unit's system time so that both contain the same time period. The correct time period is necessary to verify that the token password code that is being used by a user is valid.
- If you have more than one FortiToken device, you must enter each one in *User > FortiToken > FortiToken*; then select each one in the list and for each one activate and synchronize. FortiOS does not support the activation and synchronization of multiple FortiTokens at one time. For example, you cannot select four FortiTokens and then select *Activate* and immediately after select *Synchronization*.

The FortiToken works with two-factor authentication in the following way:

- FortiToken is assigned to a user (for example a local user in *User > User > User*)

- The user logs in with the token password code they received in an email or text message on their mobile phone

The token password code that is generated is from a seed that is unique within each FortiToken. When a user uses the correct token code for the current time period, that token code provides proof that the user is in possession of the physical FortiToken. The token code changes every 60 seconds on the FortiToken device, to prevent replay attacks. For example, a person steals some of a user's token code to reuse at a later time.

Two-factor authentication

Two-factor authentication provides a way to minimize security breaches due to stolen user credentials. Two-factor authentication requires the authenticating client to provide additional credentials beside a user name and password. You can add two-factor authentication to PKI users. SMS and Email token authentication is also supported. SSL VPN two-factor authentication supports FortiTokens.

Two-factor authentication is available for FortiGate administrators, local users and PKI users.

In *User > FortiToken > FortiToken*, the token password code from FortiToken is entered into the list by selecting *Create New*. You must activate and synchronize FortiToken so that you can use the generated token password code.

After synchronizing the token password code, you can then apply it where two-factor authentication is available within FortiOS. For example, FortiGate administrators can have the two-factor authentication enabled for their account in *System > Admin > Administrators*.

When FortiToken is used in a third-party IPsec client configuration, each user that has two-factor authentication enabled and configured must use the token password code when only a password is supported to gain access. This authentication using only a password is not supported when the password and token password code are sent in CHAP or MS-CHAP form, and the local user is authenticated using a remote server. This is because FortiOS is unable to extract back both the password and the token password code.

Example for configuring users with two-factor authentication

This example explains how to configure multiple users with the new feature two-factor authentication.

Your company requires remote access to the network for the following employees:

- two sales employees
- two employees that often work from home
- one remote FortiGate administrator for remote management

The company has purchased a FortiToken-200 for each employee that will be required to authenticate using two-factor authentication. The employees that will be logging in using two-factor authentication will be using SSL VPN. Each employee already has their own user account configured from a previous setup. You are only enabling two-factor authentication and notifying them of this new, additional log in credential.

To activate each FortiToken

- 1 Log in to the web-based manager of the FortiGate unit.
- 2 Go to *User > FortiToken > FortiToken*.

- 3 On the FortiToken page, enter the serial number of the first FortiToken, and repeat until all FortiTokens are entered.
- 4 Select *OK*.
- 5 For the first FortiToken in the list on the FortiToken page, select it and then select *Activate*.
- 6 After completing the activation, select the first FortiToken in the list and then select *Synchronization*.
- 7 Repeat steps 5 and 6 until all FortiTokens are synchronized.

The FortiTokens are now synchronized. Users can now be configured with the two-factor authentication. In the following procedure, the token password codes will be sent to users to their email accounts.

To configure employees with two-factor authentication

- 1 In the web-based manager, go to the location of the employee's account.
For example, *User > User > User*.
- 2 In the first employee's account, select *Enable Two-factor Authentication*.
- 3 Under *Deliver Token Code by*, select *FortiToken* and then select the FortiToken serial number of the FortiToken that the person will be using.
- 4 Select *Email to* and then enter the sales person's email address.
For example, *sales_1@example.com*
- 5 Select *OK*.
- 6 Repeat steps 3 and 4 to complete the rest of the employee's two-factor authentication settings.

The following procedure sends the token password code to the FortiGate administrator's mobile phone.

Enabling two-factor authentication for administrators

The new two-factor authentication is available for FortiGate administrator accounts in *System > Admin > Administrators*. Two-factor authentication is a way for you to add an additional log-in credential for users, which is a token password code. The token password code is provided by a device called the FortiToken.

FortiGate administrators with two-factor authentication must enter the token password code when logging in to the web-based manager. The token password code can be sent to the FortiGate administrator by either email or mobile phone in a text message. When an administrator with two-factor authentication first tries to log in to the web-based manager, a message similar to the following appears below *Password*.

An email message containing a Token Code will be sent to
<xxxxxx@xxxxxx.com> in a moment.

If *SMS* is enabled for sending the token password code to a mobile phone, the above message will reflect that. The administrator enters their token code in the *Token Code* field and then selects *Login*.

Figure 3: Example of an administrator who is logging in to the web-based manager for the first time who has two-factor authentication

To configure the FortiGate administrator with two-factor authentication

- 1 In the web-based manager, go to *System > Admin > Administrators*.
- 2 Edit a FortiGate administrator account.
- 3 In the Edit Administrator page, select *Enable Two-factor Authentication*.
- 4 Under *Deliver Token Code by*, select *FortiToken* and then select the FortiToken serial number that the administrator will be using.
- 5 Select *SMS*.
- 6 Select the mobile provider from the drop-down list beside (*Mobile Provider*).
- 7 Enter the FortiGate administrator's phone number in the field beside (*Phone Number*).
- 8 Select *OK*.

A text message containing the token password code is sent to their phone.

Multiple authentication group enforcement

Previously, when a user belonged to multiple user groups, this user could only access the group services that were within one group. With the multiple group enforcement feature, a user can now access the services within the groups that the user is part of. For example, userA belongs to user_group1, user_group2, user_group3, and user_group4; userA can access services within user_group1, user_group2, user_group3, and user_group4.

This feature is available only in the CLI and is enabled by default. The new command for this feature is `auth-multi-group` and checks all groups a user belongs to for firewall authentication. This new command is found in `config user settings`.

Dynamic Profiles

The Dynamic Profile feature, previously only found in FortiOS Carrier, is now available for all FortiGate models. Using the dynamic profile feature a FortiGate unit can dynamically assign a UTM profile group to a user authenticated with a RADIUS server. Dynamically assigning a UTM profile group means you can dynamically assign different levels of UTM inspection, web access and other UTM features. For information about dynamic profiles, see the [Authentication](#) chapter of the [FortiOS Handbook](#).

Hard-timeout enhancement

The new authentication hard-timeout feature ensures that users will always need to authenticate whenever their time expires. The timeout behavior is configured in the following ways:

- When the timeout behavior is set to be a hard timeout, this option forces all of the user's sessions to immediately end when the authentication timeout expires. This causes the user to re-authenticate.
- When the timeout behavior is set to be a hard timeout new sessions, this option keeps all existing sessions but forces new sessions on the same user, which that user then has to re-authenticate.

The following are the new commands you can use to configure authentication hard-timeout.

```
config user setting
  set auth-timeout <number_minutes>
  set auth-timeout-type {idle-timeout | hard-timeout | new-session}
end
```

PKI certificate authentication enhancement

PKI certificate authentication now supports the extraction of the user name from within the UPN field. This extraction allows users to log in without having to enter their user name.

This enhancement is available only in the CLI. The command syntax is as follows:

```
config user peer
  edit <peer_name>
    set ldap-mode {password | principal-name}
end
```

The `principal-name` value extracts the user name from within the UPN field.

An option for “user group matching” is available in the `config user group` command as well. This option allows you to configure authentication to match PKI user groups. The command syntax to configure this feature is as follows:

```
config user group
  edit <group_name>
    config match
      edit <group>
        set server-name <server_name>
        set group-name <group_name>
```

The following is an example of how to configure this user group matching feature.

```
config user group
  edit sslvpn
    set sslvpn-portal full-access
    set member vmlg test
    config match
      edit 1
        set server-name vmlg
        set group-name
          cn=Internet,ou=test,dc=ay,dc=fortinet,dc=com
      next
      edit 2
        set server-name test
```



```
        set group-name
            CN=qa, OU=T1359, DC=AY, DC=FORTINET, DC=COM
        end
    end
end
```

NTLM authentication enhancements

There are two enhancements for NTLM, one for guest profile access and one for inspection of initial HTTP-User-Agent values. These two enhancements are configured in the CLI. The new commands are `ntlm-guest {enable | disable}` and `ntlm-enabled-browsers <browser_name>`, which are available under the `config firewall policy` command.

The `ntlm-guest` command provides guest access to users who fail NTLM authentication. The `ntlm-enabled-browsers` command allows users to access non-supported browsers without a prompt beforehand.

NTLM authentication is essentially enabled when you configure FSSO and enabled NTLM in the identity-based security policy. Any users and user groups associated with the security policy will use NTLM to authenticate without further configuration.

New PCI Compliance Features

FortiOS 4.0 MR3 improves PCI compliance support by enhancing WiFi rogue AP detection, adding Rogue AP suppression and enhancing Endpoint security features. For information about Rogue AP features, see [“Rogue AP detection and reporting” on page 26](#) and [“Rogue AP Suppression” on page 26](#).

Endpoint Security enhancements

In FortiOS 4.0 MR3 Endpoint NAC has been renamed Endpoint Control and is available on the web-based manager from *UTM Profiles > Endpoint Control* you can configure endpoint security profiles, view the Endpoint Security application database, and work with FortiClient installers. From *UTM Profiles > Monitor > Endpoint Monitor* you can perform endpoint monitoring.

Endpoint profiles include the warn option, which displays a “block” page but allows a user to choose to continue or not, as well as sends the information back to the client. Previously, when the FortiGate unit blocks a client, the unit quarantines the user but no information was sent back to the client. With this new option, within FortiClient, you can view a list of applications that the FortiGate unit requested, any applications that caused the client to be blocked by the unit, and any applications that cause a user to continue on even though a “block” page was triggered.

The *Client Installers* submenu provides information regarding FortiClient installation, version enforcement, and FortiGuard availability for updating to a recent FortiClient Endpoint versions. The *Profile* submenu provides configuration settings for endpoint profiles which are then applied to firewall policies. The settings within application sensor were merged into the settings that are available in the Profile submenu.

Network Vulnerability Scan

The Network Vulnerability Scan feature provides more granularity and options for network scanning. Network vulnerability scanning now includes Asset Definition, Scan Schedule and Vulnerability Result. You can access the network vulnerability scanner from *UTM Profiles > Vulnerability Scan*.

Asset Definition

The Asset Definition menu allows adding ranges, discovering assets or start scans. Ranges can easily be added by selecting *Create New* on the Asset Definition page. Assets are still configured the same as they were previously, but you can now add an IP address range to be scanned.

When a scan is being performed, the activity icon in the Scan Activity column displays the progress. The scan's results appear in the Discovered Hosts for <network> window. You can scroll down the list to view all discovered assets.

Scan Schedule

The Scan Schedule menu allows you to see the status of a scan (or to start a scan), the schedule settings, the type of vulnerability scan mode, and advanced settings as well. The scheduled scan applies to all assets or asset groups that are currently enabled.

The types of scans that you can schedule are quick, standard and full. Quick scanning examines a set of the most commonly used ports for vulnerabilities. Standard scanning examines a larger number of application ports, covering many known applications. This scanning covers TCP, Service Discovery and OS Discovery but UDP is disabled.

The full scan scans the full port range 1-65535 and looks for applications running on non-standard ports, examining them for vulnerabilities.

The advanced options that are available are as follows:

- *Enable TCP Port Scan*
- *Enable Service Detection*
- *Enable OS Detection*
- *Enable UDP Port Scan*

When a scan is processing, the following occur:

- All Host assets are discovered as specified in the asset definition
 - All discovered hosts are scanned for the configured sensors, port scans and so on.
- all IP Range assets are discovered as specified in the asset definition
 - authentication is not available, reducing scan capabilities
 - these IP ranges should be converted to Host assets as needed to perform a full scan
- scanning will run for each unique IP in the list, and up to the maximum number of IP addresses supported, per-platform.
- logs are recorded about the scanning activity

Vulnerability Result

The Vulnerability Result menu allows you to view, in both graphical and tabular form, the results of the network scan. Platforms that do not have SQL logging enabled, or no SQL logging available, will only have the graphical representation.

When viewing the table containing vulnerabilities, a table similar to the log viewer table, appears at the left side of the page.

Netscan asset authentication options

In the `config netscan assets` command, the following values are hidden when the value `addr-type` is set to `range`:

- `auth-unix`

- auth-windows
- unix-username
- unix-password
- win-username
- win-password

Feature Improvements to extend IPv6 support

Each new release of FortiOS brings more IPv6 feature support. FortiOS 4.0 MR3 is no exception. This release adds IPv6 firewall acceleration using XG2, XE2, CE4, and FE8 security processors, IPv6 support for the SSL VPN web portal, IPv6 support for firewall authentication, IPv6 support for SNMP, IPv6 over DHCP, Addition IPv6 features for OSPF NSSA (not so stubby area), and more information is displayed about IPv6 sessions in the dashboard session widget.

In FortiOS 4.0 MR3, IPv6 traffic can now be redirected for user authentication using local database, RADIUS, TACACS+, or LDAP

In this release, the IPv6 Policy page contains the option of including a section title within the IPv6 security policy list. IPv6 security policies support antivirus, web filter, email filter, DLP sensor, VoIP and ICAP UTM features. Local in security policies also support IPv6.

Top Session dashboard widget IPv6 support

The Top Session dashboard widget can now display IPv4 and IPv6 addresses. IPv6 addresses are displayed only when the *IPv6 Support on GUI* is enabled in *System > Admin > Settings*.

OSPFv3 NSSA extension

OSPFv3 NSSA now includes the `default-information-originate` and `external route summary` commands for IPv6. This helps you to configure the originating default information and the external route information for IPv6 addresses.

A `get` command was also introduced to show the OSPFv3 NSSA external LSAs in the database.

The following commands have been added to `config router ospf6`, in config area:

```
set type {regular | stub | nssa}
set nssa-translator-role {candidate | never | always}
set nssa-default-information-originate {disable | enable}
set nssa-default-information-originate-metric <integer>
set nssa-default-information-originate-metric-type {2 | 1}
set nssa-redistribute {enable | disable}
```

The following were added to the `config router ospf6` command:

```
set default-information-originate {disable | enable | always}
set default-information-metric <integer>
set default-information-metric-type {2 | 1}
set default-information-route-map {route-map-name}
```

The following were added to `config summary-address`:

```
set prefix6
set advertise {enable | disable}
set tag <tag_number>
```

The following `get` command was added: `get router info6 ospf database nssa-external`.

DHCP for IPv6

DHCP for IPv6 addresses is now supported in the CLI. DHCP IPv6 is similar to DHCP IPv4.

This release also introduces the rapid-commit option. Rapid-commit is the process whereby the DHCP client and the DHCP server use a rapid DHCP IPv6 two-message exchange. This provides a short cut and the messages that are exchanged are called the DHCP IPv6 “SOLICIT” and “REPLY” messages. The `rapid-commit` command is enabled or disabled in the CLI.

For more information about DHCP IPv6, see [RFC 3315](#).

Explicit proxy and web caching improvements

The explicit proxy feature provides additional options in this release, as well as new features, such as forwarding servers and a completely new explicit FTP proxy.

The web proxy feature also now provides two `diagnose` commands to list and clear web proxy users. The `diag wad user list` command lists existing users and the `diag wad user clear` clears all users or a specific user.

Explicit FTP proxy

An explicit FTP proxy can be configured from the web-based manager and the CLI. The explicit FTP proxy is in *System > Network > Explicit Proxy* and in the CLI it is `config ftp-proxy explicit` command syntax.

FTP users connect to the explicit proxy and then connect through the proxy to remote FTP servers.

To enable the explicit FTP proxy go to *System > Network > Explicit Proxy* and select *Enable Explicit FTP Proxy* and select *Apply*. Then go to *System > Network > Interface*, select the Interface on which to enable the explicit FTP proxy and select *Enable Explicit FTP Proxy*.

Enter the following command to enable the explicit FTP proxy from the CLI:

```
config ftp-proxy explicit
  set status enable
end
```

Enter the following command to enable the explicit FTP proxy on the internal interface:

```
config system interface
  edit internal
    set explicit-ftp-proxy enable
  end
```

Once the explicit FTP proxy is enabled on an interface you must create security policies with the *ftp-proxy* as the source interface to allow explicit FTP proxy traffic. For example, to allow FTP connections from the internal network to an FTP server on the Internet, enable the explicit FTP proxy on the FortiGate internal interface and add `ftp-proxy` to `wan1` security policies.

To connect to an FTP server through the explicit FTP proxy

The following steps are required when a user starts an FTP client to connect to an FTP server through the explicit FTP proxy. Any RFC-compliant FTP client can be used.

- 1 The user connects to the explicit FTP proxy by starting an FTP session with the explicit proxy. In this example, the IP address of the FortiGate interface on which the explicit FTP proxy is enabled is 10.31.101.100.

For example:

```
ftp 10.31.101.100
```

- 2 The explicit FTP proxy responds with a welcome message and requests the user's FTP proxy user name and password and a username and address of the FTP server to connect to:

```
Connected to 10.31.101.100.
220 Welcome to Fortigate FTP proxy
Name (10.31.101.100:user):
```

You can change the message by editing the FTP Proxy replacement message.

- 3 At the prompt the user enters their FTP proxy username and password and a username and address for the FTP server. The FTP server address can be a domain name or numeric IP address. This information is entered using the following syntax:

```
<proxy-user>:<proxy-password>:<server-user>@<server-address>
```

For example, if the proxy username and password are `p-name` and `p-pass` and a valid username for the FTP server is `s-name` and the server's IP address is

`ftp.example.com` the syntax would be:

```
p-name:p-pass:s-name@ftp.example.com
```



If the FTP proxy accepts anonymous logins `p-name` and `p-pass` can be any characters.

- 4 The FTP proxy forwards the connection request, including the user name, to the FTP server.
- 5 If the user name is valid for the FTP server it responds with a password request prompt.
- 6 The FTP proxy relays the password request to the FTP client.
- 7 The user enters the FTP server password and the client sends the password to the FTP proxy.
- 8 The FTP proxy relays the password to the FTP server.
- 9 The FTP server sends a login successful message to the FTP proxy.
- 10 The FTP proxy relays the login successful message to the FTP client.
- 11 The FTP client starts the FTP session.

All commands entered by the client are relayed by the proxy to the server. Replies from the server are relayed back to the FTP client.

Explicit Web Proxy Forwarding Servers (proxy chaining)

For the explicit web proxy you can configure web proxy forwarding servers to use proxy chaining to redirect web proxy sessions to other proxy servers. Proxy chaining can be used to forward web proxy sessions from the FortiGate unit to one or more other proxy servers on your network or on a remote network. You can use proxy chaining to integrate the FortiGate explicit web proxy with an already existing web proxy solution.

A FortiGate unit can forward sessions to most web proxy servers including a remote FortiGate unit with the explicit web proxy enabled. No special configuration of the explicit web proxy on the remote FortiGate unit is required.

You can deploy the explicit web proxy with proxy chaining in an enterprise environment consisting of small satellite offices and a main office. If each office has a FortiGate unit, users at each of the satellite offices can use their local FortiGate unit as an explicit web proxy server. The satellite office FortiGate units can forward explicit web proxy sessions to an explicit web proxy server at the central office. From here the sessions can connect to web servers on the Internet.

If the explicit proxy feature is enabled and configured, you can apply a web proxy forwarding server to a web proxy security policy. Applying a forwarding server to the policy is the same as applying a UTM profile or sensor; select the *Web Proxy Forwarding Server* check box and then select a forwarding server from the drop-down list.

Authentication cookie for session-based authentication of explicit web proxy sessions

When configuring a web proxy security policy, you can now include a web-proxy cookie option which reduces the amount of authentication requests to authentication servers when session-based authentication is applied using explicit web proxy. The cookie will remember the user's session, which will then be used to map to an existing user, reducing the chance to require an authentication. This feature provides better load balancing, as well as latency.

The web authentication cookie is available only in the CLI. The `web-auth-cookie` command is used to configure this feature and is within the `config firewall policy` command.



The `web-auth-cookie` command is available only when session-based authentication is enabled.

Form-based user authentication for explicit web proxy

Previously, the explicit web proxy supported authentication only through the HTTP protocol using HTTP headers. A form-based user authentication for explicit web proxy is now available, which is similar to form-based authentication for regular security policies. A form-based authentication is used when a web page is returned to a web client which the user then authenticates with his or her user name and password. These credentials are then sent through HTTP Post request.

The form-based authentication for explicit web proxy authenticates the user and then redirects the user back to their own original URL, if the user authorizes access to the URL. This authentication is available only for IP-based authentication.

Web caching in security policies

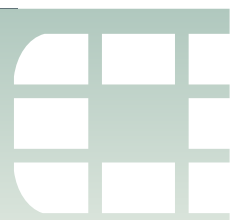
Web caching can now be enabled in a security policy. When enabled, the FortiGate unit will apply web caching to HTTP traffic accepted by the security policy. This option is available only on FortiGate units that support WAN Optimization and web caching. Enabling web caching in a security policy is similar to enabling web caching in a WAN Optimization rule. However, enabling web caching in a security policy means you can also apply UTM options to web cached traffic in a single VDOM.

You can use this option to apply web caching for explicit web proxy traffic if the Source Interface/Zone is set to the web-proxy interface. Previously, web caching was enabled as part of the explicit proxy configuration. In this release, web caching does not need to be applied to all explicit proxy traffic.

Enabling web caching in a security policy can not apply web caching to HTTPS traffic. To apply web caching to HTTPS traffic you need to create a WAN optimization rule.

Web Caching in a security policy takes place before web caching in a WAN Optimization rule. So traffic accepted by a security policy that includes web caching will not be cached by the WAN optimization rule.

Web caching supports caching of HTTP 1.0 and HTTP 1.1 web sites on the FortiGate unit hard disk. Some HTTP content accepted by the security policy may not be cached. See [RFC 2616](#) for information about web caching for HTTP 1.1.



Logging and reporting enhancements

This section describes new FortiOS 4.0 MR3 Log and Reporting features including:

- FortiGuard Analysis and Management Service (FAMS)
- The FortiGate UTM Weekly Activity Report
- Log Access Improvements
- SQL logging enabled by default
- Sending DLP archives to multiple FortiAnalyzer units
- Remote logging configuration enhancements
- Log and Report Monitoring
- Log Message Enhancements
- SSL connection encryption level option over OFTP
- Uploading logs to a FTP server in text format
- Deleting all local logs, archives and user-configured report templates

FortiGuard Analysis and Management Service (FAMS)

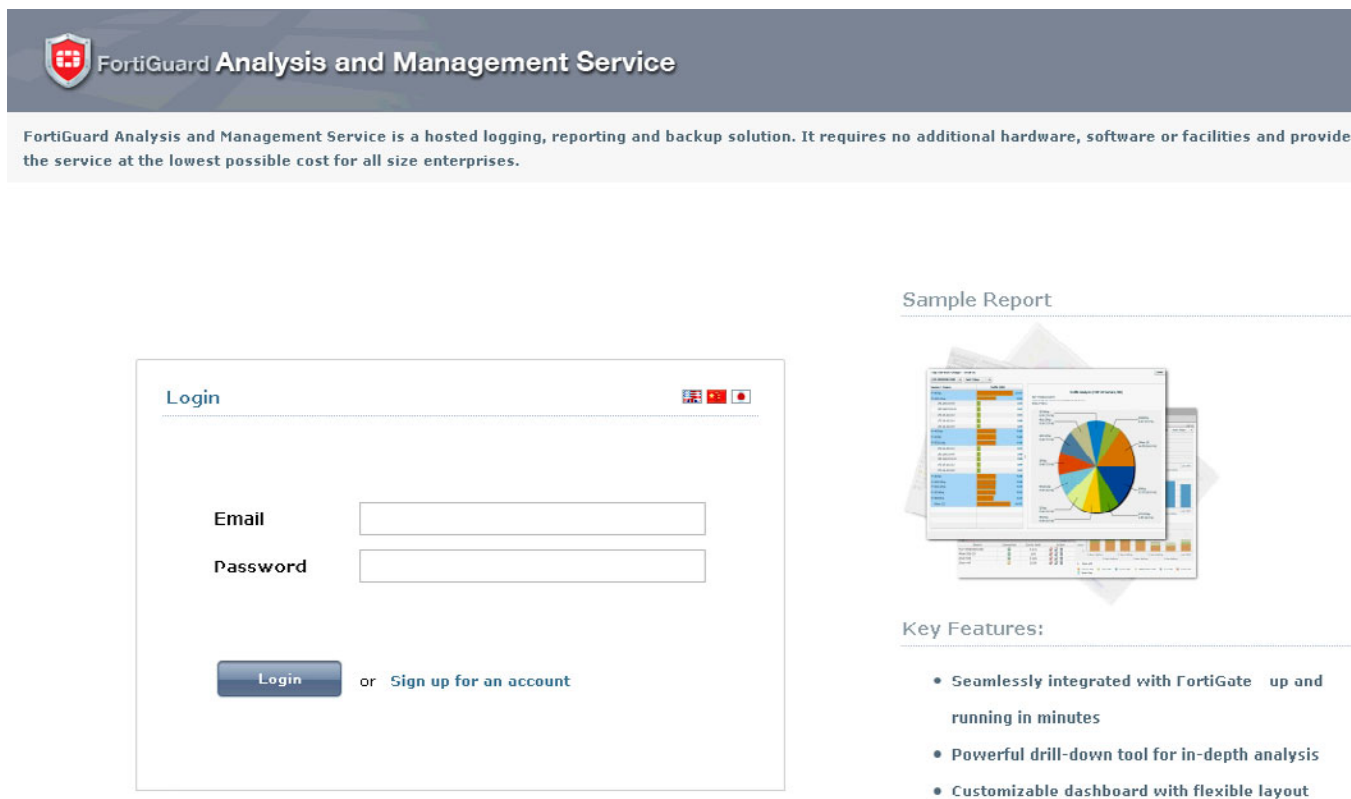
FAMS is a secure and simple offsite/hosted cloud based security management & storage product that FortiGate users can use for:

- Storing FortiGate log messages in a log message repository (default capacity 1GB per device. Additional Storage Top-ups are available with annual subscriptions)
- Custom reporting and analysis based on FortiGate log messages
- Real-time FortiGate monitoring and alerting using SNMP
- Backing up and restoring your FortiGate configuration

FAMS is available for all FortiGate models. For low-end FortiGate models FAMS is the default reporting device. You can also use a FortiAnalyzer unit as the reporting device.

You can access FAMS reports directly from your FortiGate unit once FAMS has been activated on it. You can also access the FAMS portal by logging into the FAMS portal at <https://fams.fortinet.com>.

Figure 4: FAMS portal



Communication between FortiGate units and FAMS is encrypted using SSL over TCP ports 443, 514, and 541.

If all of the FAMS storage space for your FortiGate is used, FAMS stops accepting new log messages for that FortiGate unit. You can log into the FAMS portal to free up space or you can configure FAMS to automatically remove old data after a configured storage time.

This section describes:

- [Adding FortiGate units to FAMS](#)
- [Sending log messages to FAMS](#)
- [Viewing FAMS reports from a FortiGate unit](#)

Adding FortiGate units to FAMS

To use FAMS you must register your FortiGate unit on the Fortinet support site.

Then you can activate FAMS for your FortiGate unit from the FortiGate License Information dashboard widget. To activate the FortiGate unit, select the *Activate* button.

The first time you activate a FortiGate unit with a FAMS account, select *Create Account* and create the new FAMS account by entering the email address and password of the Fortinet support account used to register the FortiGate unit.

To add more FortiGate units to an already created FAMS account, select *Existing Account* and enter the email address and password of the support account used to register the FortiGate unit.

All FortiGate units added to a FAMS account must be registered with the same support account.

License Information	
Support Contract	
Registration	Registered (Login: techdoc@fortinet.com) [Login Now] ✓
Hardware	8 x 5 support (Expired: 2012-02-13) [Renew] ✕
Firmware	8 x 5 support (Expired: 2012-02-13) [Renew] ✕
Enhanced Support	24 x 7 support (Expired: 2012-02-13) [Renew] ✕
Comprehensive Support	24 x 7 support (Expired: 2012-02-13) [Renew] ✕
FortiGuard Services	
AntiVirus	Expired [Renew] ✕
IPS	Expired [Renew] ✕
Vulnerability Scan	Expired [Renew] ✕
Web Filtering	Not Registered [Configure] ✕
Email Filtering	Not Registered [Configure] ✕
FAMS	
Status	Activate ✕
Virtual Domain	
VDOMs Allowed	10
FortiClient Software	
FortiClient	Unlicensed [Enter License] ✕
FortiClient Connections 0 / 10	

Activate FAMS

Existing Account Create Account

Please enter the information below and click the Activate button.
Warning! Activating FAMS will disable logging to FortiAnalyzer.

Email:

Password:

Each FortiGate unit gets 1GB of FAMS storage. You can buy annual subscriptions for more storage if you need it.

Sending log messages to FAMS

Once you have activated FAMS for a FortiGate unit you can use the following steps to send log messages from your FortiGate unit to FAMS. Once this is set up, all log messages will be sent to FAMS.

- 1 Go to *Log & Report > Log Config > Log Setting*.
- 2 Select *Upload logs remotely > FAMS*.
- 3 Select *Apply*.

- 4 You can select TEST CONNECTIVITY to verify that the FortiGate unit can connect to FAMS.



To stop saving log messages on the FortiGate unit you can clear the Disk or Memory selections.

Viewing FAMS reports from a FortiGate unit

Once you have activated FAMS for a FortiGate unit and configured logging to FAMS you can go to *Log & Report > FAMS > Report* to view and customize reports created by FAMS from your FortiGate unit's log messages.

Logging performance optimization for FortiOS 4.0 MR3 patch 7

There have been some significant changes introduced in FortiOS v4.0 MR3 Patch 7 to reduce the performance cost of local logging (logging to disk or memory).

In previous releases when logging to FortiAnalyzer in real time, log messages were first saved to the FortiGate log disk before being sent to the FortiAnalyzer unit and you could not disable local logging.

FortiAnalyzer real time logging no longer requires disk logging

FortiAnalyzer real-time logging no longer requires saving log messages to the FortiGate log disk resulting in improved performance because CPU and memory resources are not being used to store log messages on the log disk. (Saving log messages to the log disk uses system memory for I/O caching).

To take advantage of this change, after upgrading to Patch 7, you can enable FortiAnalyzer real time logging and disable local disk-logging using the following command:

```
config log fortianalyzer setting
  set upload-option realtime
end
```

Then disable disk logging:

```
config log disk setting
  set status disable
end
```

SQL database moved from the log disk to system memory for some models

For FortiGate-100D and FortiGate-300C units, the SQL logging database has been moved from local storage to a filesystem in RAM memory (about 10% of system memory is available for the SQL database). No configuration changes are required.

Disabling extended traffic logging

Extended traffic logging is required for ICSA compliance and is enabled by default independantly of other traffic log settings. When enabled, traffic log message volume is doubled because a log message is generated when a sessions starts and another one is generated when the session ends. When extended traffic logging is disabled, a single log message is generated when a session stops.

Extended traffic logging also causes traffic hitting a deny policy (or the implicit deny policy) to be logged even if traffic logging is disabled for the deny policy.

Extended traffic logging also generates log messages for:

- All dropped ICMP packets
- All dropped invalid IP packets

Extended traffic logging is not rate limited. A large volume of invalid packets can dramatically increase the number of log entries.

Use the following command to disable extended traffic logging for FortiAnalyzer logging:

```
config log fortianalyzer filter
    set extended-traffic-log disable
end
```

Use the following command to disable extended traffic logging for disk logging:

```
config log disk filter
    set extended-traffic-log disable
end
```

Reducing SQL logging database size

When SQL logging is available on a FortiGate unit, memory usage related to SQL logging I/O can be reduced by keeping the SQL database file as small as possible.

Set the maximum SQL database file size using the following command. Set it at minimum size to reduce memory usage. The size range is 512 MB to 65536 MB and the default size is 1024 MB:

```
config system global
    set max-sql-log-size 512
end
```

Then rebuild the SQL database:

```
# exec log recreate-sqldb
This will recreate the SQL log database.
All local logs recorded with SQL logging will be deleted!
Do you want to continue? (y/n)y
SQL log database is being recreated in the background.
```

Disable SQL logging filters on the local disk

You can reduce log disk I/O overhead by disabling SQL logging filters.

```
config log disk setting
    config sql-logging
        set app-ctrl disable
        set attack disable
        set dlp disable
        set netscan disable
        set spam disable
        set traffic disable
        set virus disable
        set webfilter disable
    end
```

Disable SQL logging on AMC disk models (ASMS08)

Avoid using SQL logging with AMC module disk. This feature is disabled by default and you can use the following command to disable it if it was previously enabled:

```
config system global
    set sql-logging disable
```

```
end
```

The FortiGate UTM Weekly Activity Report

The FortiGate UTM Weekly Activity Report is available on FortiGate units with hard disks if logging to disk is enabled by going to *Log&Report > Log Config > Log Setting* and selecting Disk Logging and Archiving. When you enable Disk logging you can go to *Log&Report > Report Access* to view the FortiGate UTM Weekly Activity Report. You can browse through the sections of this report to view current bandwidth and application usage, web usage, email usage, threats, and VPN usage.

The data for the report is generated by saved SQL logging messages. By default logging to disk and SQL logging are enabled and the report is produced. If logging to disk is disabled the report does not appear. If logging to disk is enabled and SQL logging is not enabled the report appears but will not contain any data. If some report data appears and some does not the cause could be that only some types of SQL logging are enabled.

SQL logging is only enabled and configured from the CLI. Use the following command to enable SQL logging:

```
config log disk setting
  set status enable
config sql-logging
  set app-ctrl enable
  set attack enable
  set dlp enable
  set event enable
  set netscan enable
  set spam enable
  set traffic enable
  set virus enable
  set webfilter enable
end
end
```

By default the UTM Weekly Activity Report is generated and saved weekly and from any report access page you can select Historical Reports to view previously generated reports. From the Historical reports list you can also download the reports in PDF format and delete them.

You can modify the default FortiGate UTM Weekly Activity Report to meet your requirements from any report page by selecting *Edit*. When you select *Edit*, the page refreshes in Editing mode. In editing mode can change the content and the appearance of the report pages, change the data displayed on individual report pages and add or delete report pages.

A modified report must be saved using the Save icon. Any modifications that are not saved, are lost.

A report consists of text, charts and images. Text elements are used to add titles and descriptive text to the report. Images are used to add graphics to the report. Charts and used to add text and graphical data to the report. You can add a bar chart, line chart, pie chart and table chart. When you add a chart you can customize its appearance as well as the data that the chart displays. To customize the data displayed you can choose for hundreds of predefined reports. Each report includes formatting settings and settings to extract data from the FortiGate log database.

FortiOS 4.0 MR3 includes the following new reports:

- traffic.bandwidth.apps.app_cat
- traffic.bandwidth.app_cats.user
- traffic.bandwidth.users
- traffic.sessions.apps.app_cat
- traffic.sessions.app_cats.user
- traffic.sessions.users
- traffic.bandwidth.apps.user
- traffic.bandwidth.users.app
- traffic.bandwidth.app_cats
- traffic.sessions.apps.user
- traffic.sessions.users.app
- traffic.sessions.app_cats
- traffic.bandwidth.wanopt
- web.allowed-request.sites.user
- web.allowed-request.users.web_cat
- web.allowed-request.web_cats
- web.blocked-request.sites.user
- web.blocked-request.users.web_cat
- web.blocked-request.web_cats
- web.requests.phrases.user
- web.requests.users.phrase
- web.requests.phrases
- web.allowed-request.users.site
- web.allowed-request.sites
- web.blocked-request.users.site
- web.blocked-request.sites
- web.bandwidth.sites.user
- web.bandwidth.users.site
- web.bandwidth.sites
- web.bandwidth.stream-sites.user
- web.bandwidth.users.stream-site
- web.bandwidth.stream-sites
- email.request.timeperiods.sender
- email.request.senders
- email.bandwidth.timeperiods.sender
- email.bandwidth.senders
- email.request.timeperiods.receiver
- email.request.receivers
- virus.count.viruses.user
- virus.count.users.virus

- virus.count.viruses
- virus.count.users
- virus.count.viruses.protocol
- virus.count.protocols
- attack.count.critical-attacks.user
- attack.count.users.critical-attack
- attack.count.critical-attacks
- attack.count.attacks.user
- attack.count.users.attack
- attack.count.attacks
- vpn.bandwidth.static-tunnels.user
- vpn.bandwidth.users.static-tunnel
- vpn.bandwidth.static-tunnels
- vpn.bandwidth.ssl-sources.user
- vpn.bandwidth.users.ssl-source
- vpn.bandwidth.ssl-sources
- vpn.bandwidth.dynamic-tunnels.user
- vpn.bandwidth.users.dynamic-tunnel
- vpn.bandwidth.dynamic-tunnels

Viewing the current and historical reports

Going to *Log&Report > Report Access* you can view current data in the FortiGate UTM Weekly Activity Report.

You can also select *Historical Reports* to view previously generated FortiGate UTM Weekly Activity Reports. When you select *Historical Reports* on the Viewing default layout page, you are automatically redirected to the Historical Reports page where you can view, download, and delete generated reports.

Historical Reports page	
Lists all generated reports. You can remove generated reports from this page or return to the previous page, the Viewing default layout page.	
Return to Layout	When selected, you are automatically redirected to the Viewing default layout page.
Delete	Removes a report from within the list. To remove multiple reports from within the list, on the page, in each of the rows of the reports you want removed, select the check box and then select <i>Delete</i> . To remove all reports from the list, on the page, select the check box in the check box column, and then select <i>Delete</i> .
Report File	The report name that the FortiGate unit gave the report. This name is in the format <scheduletype>-<report_title>-<yyyy-mm-dd>-<start_time>. For example, Once-examplereport_1-2010-09-12-103044, which indicates that the report titled examplereport_1 was scheduled to generate only once and did on September 12 at 10:30 am. The hour format is hh:mm:ss.

Started	The time when the report began generating. The format is yyyy-mm-dd hh:mm:ss.
Finished	The time when the report finished generating. The format is yyyy-mm-dd hh:mm:ss.
Size (bytes)	The size of the report after it was generated. The size is in bytes.
Other Formats	The other type of format you chose the report to be in, for example PDF. When you select PDF in this column, the PDF opens up within the page. You can download the PDF to your local PC from this page as well.

Creating custom reports from the CLI

You can add additional reports from the CLI by adding datasets, charts, layout, style, summary, and themes for reports; however, these options are available only from the CLI. When you add a report from the CLI the report layout does not appear on web-based manager. You can review historical reports for CLI-configured reports in the same way as FortiGate UTM Weekly Activity Reports.

Log Access Improvements

The Log & Archive Access menu contains the following changes to existing features, as well as support for downloading log messages directly from the FortiGate unit to your PC.

- [Viewing log messages](#)
- [Filtering log messages](#)
- [Downloading log messages](#)

Viewing log messages

When you are viewing log messages within the Log & Archive Access menu, you will find detailed information about the log messages at the bottom of the page. For example, you are viewing event log messages in *Log&Report > Log & Archive Access > Event*, and you see the first log message, in detail, in a table below the *Log location*: *<log_storage_device>* and page controls.

By selecting the down arrow beside *Detailed Information*, you can view this detailed information about log messages either at the bottom of the page, or on the right side of the page. You can also select *Hidden*, which hides the table.

Figure 5: Viewing event log messages with the default Bottom viewing option selected

#	Date	Time	Level	Sub Type	ID	User Interface	Action	Message
1	2011-02...	11:01:...	informati...	admin	320...	http(172.20.120.23)	login	Administrator admin logged in successfully from http(172.20.120.23)
2	2011-02...	10:59:...	informati...	admin	320...	http(172.20.120.23)	logout	Administrator admin logged out from http(172.20.120.23)
3	2011-02...	10:59:...	alert	admin	324...	jsconsole		Configuration is changed in the admin session
4	2011-02...	10:59:...	informati...	admin	320...	jsconsole	logout	Administrator admin logged out from jsconsole
5	2011-02...	10:23:...	informati...	admin	321...			interface wan1 gets a DHCP lease, ip:172.20.120.231, mask:255...
6	2011-02...	09:55:...	informati...	dhcp	260...			Client requests IP address/configuration parameters
7	2011-02...	09:55:...	informati...	dhcp	260...			Client requests IP address/configuration parameters
8	2011-02...	09:55:...	informati...	dhcp	260...			Client requests IP address/configuration parameters
9	2011-02...	09:55:...	informati...	dhcp	260...			Client requests IP address/configuration parameters
10	2011-02...	09:55:...	informati...	dhcp	260...			Client requests IP address/configuration parameters
11	2011-02...	09:55:...	informati...	dhcp	260...			Client requests IP address/configuration parameters
12	2011-02...	09:55:...	informati...	dhcp	260...			Client requests IP address/configuration parameters
13	2011-02...	09:49:...	informati...	dhcp	260...			Client requests IP address/configuration parameters
14	2011-02...	09:39:...	notice	auth	430...	UNKNOWN(2.2.2.2)		forticlient msg
15	2011-02...	09:39:...	notice	auth	430...	UNKNOWN(2.2.2.2)		forticlient msg

Log Location: Disk			
Date	2011-02-04	Time	11:01:13
Level	information	Sub Type	admin
ID	32001	User	admin
User Interface	http(172.20.120.23)	Action	login
Status	success	Reason	none
Profile Name	super_admin	Message	Administrator admin logged in successfully from http(172.20.120.23)

At the bottom of the list of logs on the page, before page controls, the *Log location*: `<log_storage_device>` indicates where the logs are being stored, such as the local hard disk or memory.

Filtering log messages

Previously, when filtering log messages, you had to select the Filter icon within each column and then indicate the information that you wanted filtered. You can now use *Filter Settings*, providing an easier way to filter the information on the page without using the Filter icons. The Filter icons still indicate if filtering is enabled for that column.

Downloading log messages

Log messages can now be downloaded in Raw format directly from within the Log Access menu. For example, in *Log&Report > Log & Archive Access > Event*; within the Event page, select *Download Raw Log*.

All log messages, including archived log messages, can be downloaded from the FortiGate unit to the management computer at any time. The downloaded file is a text file, which can be viewed on a text editor, such as Notepad. The log file name is in the format `<log name><number>.log`. For example, `elog0101.log`. The last number changes to reflect the log type number, such as DLP, which is nine (for example, `dlog0109.log`).

New Unified UTM Log Access

The new UTM Log submenu in *Log&Report > Log & Archive Access > UTM Log* provides a central location for all UTM-related log messages. These include virus, attack, DLP, application control, email filter, and web filter log messages. On the UTM Log access page includes a new column called *UTM Type* which indicates if the UTM feature that generated the log message.

Figure 6: The UTM page in *Log&Report > Log Access > UTM*

#	Date	Time	Level	Sub Type	ID	UTM Type	Message	Src	Dst	User	Src Port	Dst Port	Packet Log
1	2011-0...	09:36:15	warning	infected	8192	AntiVirus	File is infect...	1.1.1.1	2.2.2.2		2560	5120	
2	2011-0...	09:36:15	warning	filename	0440	AntiVirus	File is blocke...	1.1.1.1	2.2.2.2			5120	
3	2011-0...	09:36:15	warning	ftpd_bk	13056	Web Filter		1.1.1.1	2.2.2.2	user	2560		
4	2011-0...	09:36:15	alert	signature	16384	Attack	N/A			user	2560	5120	
5	2011-0...	09:36:15	notice	smtp	20480	Email Filter		1.1.1.1	2.2.2.2	user	2560		
6	2011-0...	09:36:15	warning	dlp	24576	DLP		1.1.1.1	2.2.2.2	user			
7	2011-0...	09:36:15	informat...	app ctrl-all	28672	Application Co...				user		5120	

Log location: Disk	
Date	2011-01-27
Time	09:36:15
Level	warning
Sub Type	infected
ID	0192
Message	File is infected.
Status	passthrough
Service	mm1
Src	1.1.1.1
Dst	2.2.2.2
Src Port	2560
Dst Port	5120
Src Interface	lu
Dst Interface	eth0

When viewing logs in Raw format, the downloaded UTM log file is called ulog and contains all the UTM-related log types, such as virus and attack. There is no log field called UTM Type in the log message when viewing them in the Raw format. The type and subtype fields indicate which log file the log message is associated with. For example, type=virus and subtype=filename.

SQL logging enabled by default

SQL is not enabled by default on models with an internal hard disk, such as a FortiGate-60C, as well as models with a removable hard drive when the disk is inserted into the FortiGate unit.

After upgrading to this release, a window appears when logging into the web-based manager. In the window, you can enable SQL logging when you select Go. This option does not immediately send logs to the FortiGate unit's local hard disk or removable hard disk; traffic must be flowing through the unit as well as UTM profiles and/or sensors applied to security policies.

The window appears when both the following are present:

- the model contains an internal or removable hard disk
- no SQL logging options are enabled

If you decide you would rather enable SQL logging later, select Remind me Later, which will prompt you when you log into the web-based manager again.

When SQL is enabled from the window, the FortiGate unit converts an previous logs to SQL format, and all log categories are that were previously enabled for disk logging are written in SQL format.

Sending DLP archives to multiple FortiAnalyzer units

When configuring multiple FortiAnalyzer units, you can now include sending DLP archives to both the second and third FortiAnalyzer units. This enhancement allows you to ensure DLP archives are not lost when logging to multiple FortiAnalyzer units.

Remote logging configuration enhancements

Remote logging to a log device is now configured mostly in the CLI, except you can configure uploading logs to a FortiAnalyzer unit or FAMS in either the CLI or web-based manager. However, you must configure when to upload the logs from the CLI, since the time period is not supported in the web-based manager until after the time period is configured in the CLI.

SQL logging is enabled by default for those models that have SQL databases. If you want to disable or enable certain SQL logs, including archiving, you must use the CLI.

Figure 7: Log settings in FortiOS 4.0 MR3

When configuring logging to a FortiAnalyzer unit, you can control the buffer rate to the FortiAnalyzer unit. This is available only in the CLI. The buffer size is between 20 to 20 000.

Previously, you could upload logs to an AMC disk; however, this feature has been removed because of the new feature of remotely storing and uploading logs to a FortiAnalyzer unit and FAMS server.

Log and Report Monitoring

The new Monitor submenus allow you to view monitored network activity on the FortiGate unit. In *Log&Report > Monitor > Logging Monitor*, you can view the log activity being recorded by the FortiGate unit on a weekly basis.

Logging Monitor

The Logging Monitor allows you to view the log activity that is being recorded by the FortiGate unit. The information displays as a bar chart and contains information regarding the total number of logs recorded by the unit on each day of the week. For example, on Wednesday of this week there were a total of 30 log entries recorded by the event log.

When you select a bar in the bar chart, you are automatically redirected to the Log Activity for <day of week> page. On this page you can view the logs for that day and the number of entries for that log file that occurred. For example, you select Wednesday's bar on the Logging Monitor page; you are redirected to the Log Activity for Wednesday page, where the logs for that day display. When you want to return to the Logging Monitor page, select *Return*.

Log Message Enhancements

There are several enhancements, as well as changes, that occurred for logs in this release. For example, event logs contain a new subtype called DNS.

This topic includes the following:

- [Event logs](#)
- [Other-traffic logs](#)
- [Chat message log support for MSNP21](#)



In antivirus logs, the URL address now states the type of protocol used instead of always using "http://". For example, in an ftp-over-http traffic log, the URL starts with ftp://.

Event logs

There are two new subtypes that have been added to the event log file, config and dns. The following explains each one.

A new subtype was added to event logs, called DNS. This new log message provides information about any DNS look-up that occurred. The option is enabled within the Event Log page (*DNS lookup event*), or within the CLI.

There is only one log message that occurs within the event log.

The following is an example of an event-dns log message.

```
2010-08-13 20:05:43 log_id=0108050000 type=event subtype=dns
vd=root pri=information policyid=1 src=172.16.120.166
dst=10.10.1.10 src-intf="internal" dst_intf="wan1" user="user1"
group="group123" dns_name="xx.example.com" dns_ip="172.55.154.199"
```

The event-config log messages provides detailed information about what setting was changed by a user. For example, a user disabled the explicit web proxy event on the Event Log page.

You can enable this subtype within the Event Log page, by selecting *Configuration change event*, or in the CLI. By default, this option is disabled.

The following is an example of an event-config log message:

```
2010-09-15 10:15:55 log_id=010 type=event subtype=config vd=root
pri=information vd=root user="admin" ui="GUI(10.10.10.1)"
action="edit" cfg_tid=1179790 cfg_path="log.eventfilter"
cfg_attr="wan-opt[enable->disable]" msg="Edit log.eventfilter"
```

Within the event log file, a log message containing information about an explicit web proxy event is recorded when enabled in *Log&Report > Log Config > Event Log*. The check box beside *Explicit web proxy event* must be selected so that this log can be recorded by the unit. This option is also available in the CLI.

Event-system

There are now two specific log messages that indicate when the system starts up and when it shuts down. These log messages are included in the event-system logs, and log message 20202 indicates when the system started up, and log message 20203 indicates when the system shut down.

The following are examples of these two event-system log messages:

```
2010-09-12 10:24:02 log_id=0100020203 type=event subtype=system
vd=root pri=information action=daemon-shutdown daemon=getty pid=68
msg= "Daemon getty shut down"
```

```
2010-09-12 10:24:02 log_id=0100020203 type=event subtype=system
vd=root pri=information action=daemon-startup daemon=cauploadd
pid=94 msg "Daemon cauploadd started."
```

Traffic logs

There are two new enhancements for traffic logs. Additional information has been added to other-traffic logs and a new subtype introduced. The new webproxy-traffic subtype for traffic logs indicates activity regarding web proxy traffic that was detected using a web-proxy security policy.

Other-traffic logs

When viewing other-traffic logs in the web-based manager, you will see additional information such as IM and P2P application information, as well as two icons in the status field that indicate the status of the traffic logs of 6 and 5. The status icons that appear in the web-based manager are a green check mark or a circle with a line through it. When you move your mouse over the icon, it indicates what the icon is, either *accept* (which is the green check mark), or *deny* (the circle with a line through it).

Chat message log support for MSNP21

In Windows Live Messenger 2011, a new protocol was introduced called Microsoft Notification Protocol 21 (MSNP21) which handles chat messages. The FortiGate unit now supports logging of chat messages that use this new protocol.

The FortiGate unit detects the protocol by following the same path as previously for IM logging. These logs are found in the DLP archive logs.

SSL connection encryption level option over OFTP

The SSL connection encryption level option for SSL connections that occur over OFTP, such as FortiGate to FortiAnalyzer, is now available. This type of connection provides a way to customize the level of SSL encryption over OFTP for these connections.

The commands are as follows:

```
config log fortianalyzer setting
  set enc-algorithm {default | high | low | disable}
end
config log fortianalyzer2 setting
  set enc-algorithm {default | high | low | disable}
```

```
end
config log fortianalyzer3 setting
  set enc-algorithm {default | high | low | disable}
end
config log fortianalyzer override-setting
  set enc-algorithm {default | high | low | disable}
end
config log fortiguard setting
  set enc-algorithm {default | high | low | disable}
end
config system central-management
  set enc-algorithm {default | high | low | disable}
end
config log disk setting
  set upload-ssl-conn {default | high | low | disable}
end
```

When you select the `default` option, you are choosing to have the SSL communication encryption with high and medium encryption algorithms.

Uploading logs to a FTP server in text format

Logs can now be uploaded in text format to a FTP server. This provides more flexibility for saving logs in a specific format for viewing later on. This is available only for FortiGate units with hard disks and only for uploading to a FTP server.

Logs that are saved in text format can be viewed in a text editor, and these logs are in Raw format. Raw format is a type of format that displays log messages as they would appear in the log file.

Example for uploading logs to a FTP server in text format

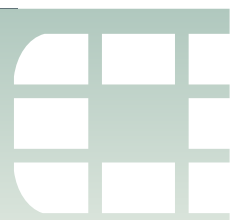
In this example, an administrator is configuring logging to the FortiGate unit's disk, as well as specifying uploading logs to an FTP server in text format.

```
config log disk setting
  set status enable
  config sql-logging
    set app-crt1 enable
    set attack enable
    set dlp enable
    set event enable
    set netscan enable
    set traffic enable
    set spam enable
    set traffic enable
    set virus enable
    set webfilter enable
  end
  set ips-archive enable
  set storage Internal
  set diskfull overwrite
  set log-quota 50
  set report-quota 50
  set upload enable
  set upload-destination ftp-sesrver
```

```
set uploadip 172.16.120.154
set uploadport 443
set uploaduser user_1
set uploadpass 123456789
set uploaddir c:\logs_fgt50B
set uploadtype appctrl attack dlp event spamfilter traffic
virus webfilter
set uploadzip enable
set upload-format text
set uploadsched enable
set uploadtime 7
set drive-standby-time 19800
set upload-delete-files disable
set sql-max-size 65536
set sql-max-size-action overwrite
set sql-oldest-entry 1024
end
```

Deleting all local logs, archives and user-configured report templates

The new `execute` command, `execute log-report reset`, deletes all local logs, log archives and user-configured report templates on the FortiGate unit. However, this command also restores the default FortiOS UTM Activity report to its original default settings, if the default report has been modified. The user-configured templates are the themes that you have configured from scratch for reports.



FortiOS 4.0 MR3 Usability improvements

A major effort has been made to improve the usability of the FortiOS 4.0 MR3 web-based manager experience. Changes have been made throughout to improve the visibility of information and make it easier and more efficient to view and change configurations and monitor network activity and FortiGate activities and processes.

This section contains the following topics:

- [High-level web-based manager menu changes](#)
- [New FortiGate Setup Wizard](#)
- [FortiExplorer enhancements](#)
- [Dashboard Widgets](#)
- [Chart display improvements](#)
- [Monitoring Improvements](#)
- [Filtering web-based manager lists](#)
- [Reference count column \(object usage visibility\)](#)
- [Configuration object tagging and coloring](#)
- [Security configuration object icons](#)
- [Access to online help](#)
- [Backing up and restoring configuration files per-VDOM](#)

High-level web-based manager menu changes

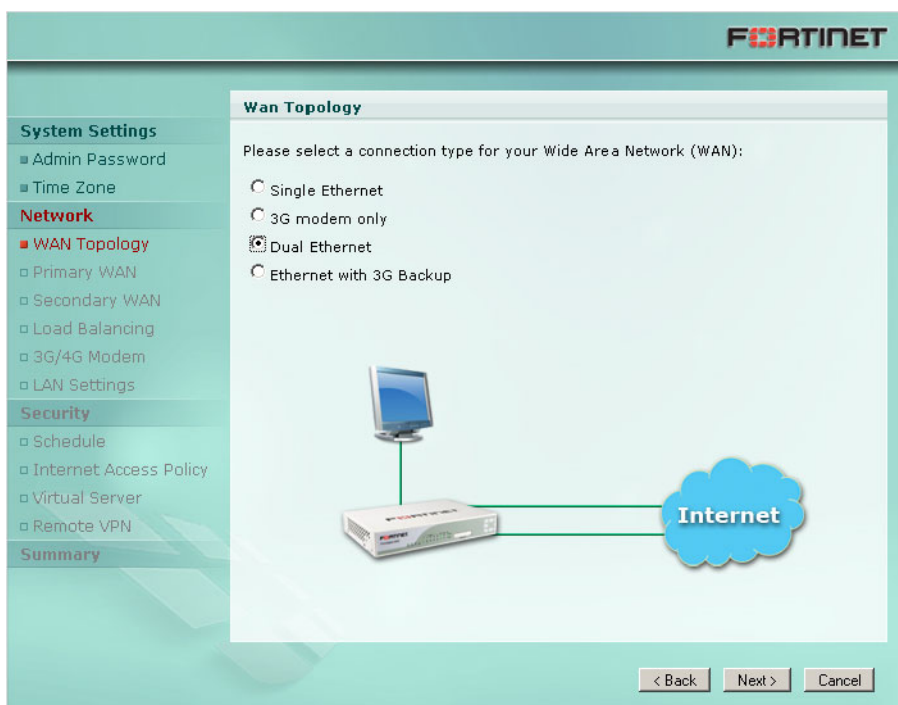
FortiOS 4.0 MR3 patch 1 introduces the following menu changes to the web-based manager. The CLI commands for these configuration items have not changed.

- The new *Policy* menu is used to configure IPv4 and IPv6 security policies, view the central NAT table, configure DoS policies, Sniffer policies, and protocol options. You can also monitor sessions and policy usage. Security policies are also called firewall policies. These options were available from *Firewall > Policy*.
- The *Firewall* menu has been renamed *Firewall Objects* and contains menus for configuring firewall addresses, services, schedules, traffic shapers, virtual IPs, firewall load balancing and monitoring load balancing and traffic shaping.
- The *UTM* menu has been renamed *UTM Profiles*.
- *Endpoint Control* and *Vulnerability Scan* have been moved under *UTM Profiles*. This functionality is now documented in the UTM Guide chapter of the FortiOS Handbook.
- The *System > Network > DNS* contains DNS fields formerly present in the *System > Network > Options* page. This page also includes DDNS settings.

New FortiGate Setup Wizard

Available on selected models, the new FortiGate setup wizard allows for quick and easy set-up of your FortiGate configuration. Within the wizard, you can configure the administrator password, FortiGate unit time zone, network settings (single or dual WAN interfaces, modem settings, DHCP and LAN settings), apply security features such as access schedules, UTM features, NAT, virtual servers, and remote SSL or IPsec VPN access.

Figure 8: Configuration wizard WAN topology setting



FortiExplorer enhancements

The most recent version of FortiExplorer is compatible with recent FortiGate models running FortiOS 4.0 MR3. You can use FortiExplorer to easily and quickly configure your FortiGate unit with basic settings. FortiExplorer also allows access to the web-based manager and CLI through a USB connection. FortiExplorer runs on all Windows platforms and on Mac OS X.

FortiExplorer contains improved setup wizard support, FortiGuard support, additional system improvements and a new security policy wizard which is similar to the FortiGate setup wizard but for security policies. FortiExplorer also contains a 3G/4G modem configuration page, for those units that have 3G/4G modem capabilities.

Dashboard Widgets

There are several enhancements to dashboard widgets in this release, as well as a new widget called Network Protocol Usage. You can view dashboard widgets from *System > Dashboard > Status*.

Traffic History

The Traffic History widget has been enhanced, allowing you to customize which line charts contain a specified time period range. For example, the second line chart displays the last seven days of traffic information.

You can choose to have the time period display in days, minutes or hours. You must enter a time period that is either in minutes or days, such as 10 minutes or 30 days. If you choose to enter zero, that specific time period is disabled.

Dashboard - Traffic History Settings	
Provides settings for modifying the default settings of the Traffic History widget.	
Custom Widget Name	Enter a new name for the widget. This is optional.
Select Network Interface	Select an interface (Fortinet unit's interfaces) from the drop-down list. The interface you choose displays the traffic occurring on it.
Enable Refresh	Select to enable the information to refresh.
Time Period 1	The time period for the first line chart. Enter a number in the first field, then select <i>Hour(s)</i> , <i>Minute(s)</i> or <i>Day(s)</i> from the drop-down list beside the field.
Time Period 2	The time period for the second line chart. Enter a number in the first field, then select <i>Hour(s)</i> , <i>Minute(s)</i> or <i>Day(s)</i> from the drop-down list beside the field.
Time Period 3	The time period for the third line chart. Enter a number in the first field, then select <i>Hour(s)</i> , <i>Minute(s)</i> or <i>Day(s)</i> from the drop-down list beside the field.

System Resources

The System Resource widget now only displays information concerning the CPU and memory usage amounts. You can view this information either in real-time or current information, or historical. If you want to view the information in historical view, you can also change the type of fill-line color.

Dashboard - Custom System Resource Display	
Provides settings to modify the default or current configuration of the System Resource widget.	
Custom Widget Name	Enter a new name for the widget. This is optional.

View Type	<p>Select which type you want to view the system resource information in.</p> <ul style="list-style-type: none"> • Real-time – displays the current information as a dial gauge, along with a percent, located at the bottom. For example, Memory Usage 58%. • Historical – displays the information in a fill-line chart for each CPU and memory. When you select <i>Historical</i>, the <i>Chart Color</i> option appears. • When viewing CPU and memory usage in the web-based manager, only the information for core processes displays. CPU for management processes, is excluded. For example, HTTPS connections to the web-based manager.
Chart Color	<p>Select <i>Change</i> to change add a new fill color to the chart. Select <i>Reset</i> to reset the color back to its default color.</p>
Time Period	<p>Select from the drop-down list, the period of time that the information will be displayed.</p>

Network Protocol Usage

The Network Protocol widget allows you to view many different protocols over a period of time. This widget reflects what was previously found in the basic traffic report, located in *Log&Report > Report Access > Memory* in FortiOS 4.0 MR1 and lower.

The Network Protocol Usage widget allows you to view many different protocols over a period of time. You can view this information with either a line chart or bar chart style. Network protocol usage information can be viewed for up to the last 30 days, or as recent as the last 24 hours.

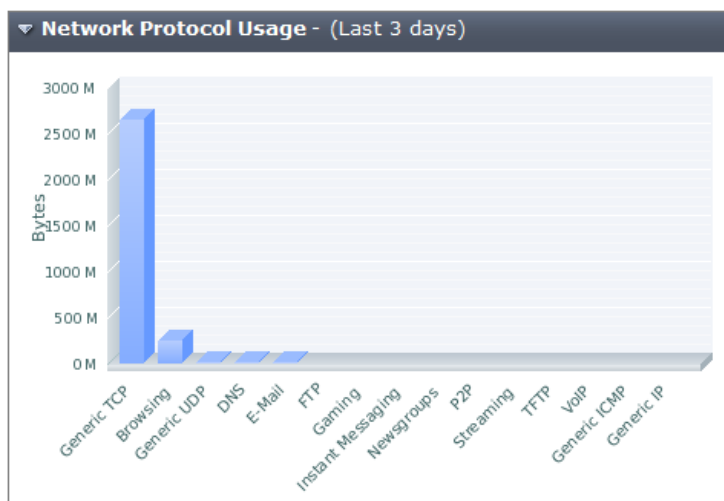
Custom Network Protocol Usage Display	
Provides settings for modifying the default settings of the Network Protocol Usage widget.	
Custom Widget Name	Enter a new name for the widget. This is optional.
Chart Style	Select either <i>Line</i> or <i>Bar</i> style for the chart. The line chart is a fill-line chart style type.
Time Period	Select a time period from the drop-down list. For example, if you choose <i>Last 24 hours</i> , only the information gathered in the last 24 hours displays.
Protocols	You can choose from any of the following protocols:
	<ul style="list-style-type: none"> • Browsing • DNS
	<ul style="list-style-type: none"> • FTP • Gaming
	<ul style="list-style-type: none"> • Newsgroups • P2P
	<ul style="list-style-type: none"> • TFTP • VoIP
	<ul style="list-style-type: none"> • Generic UDP • Generic ICMP
	<ul style="list-style-type: none"> • E-mail • Instant Messaging
	<ul style="list-style-type: none"> • Streaming • Generic TCP

	<ul style="list-style-type: none"> Generic IP
	All protocols are enabled by default. If you do not want to include certain protocols, select the check box beside each protocol that should not be included.

Chart display improvements

Charts within the web-based manager have a larger font size and chart style applied to them. These changes make it easier to read the information that displays. These chart improvements include the charts within widgets as well as within FortiOS reports.

Figure 9: Example of the display improvements to a chart



Monitoring Improvements

In each menu in the web-based manager, there is now a Monitor submenu containing one or multiple submenus that allow you to view the activity of a specific feature that is currently being monitored by the FortiGate unit. The information displayed is usually in a table or graphical format, providing a more user-friendly display of the monitored information.

The information is displayed in a similar manner as to how widgets display their information in charts or lists on a dashboard in *System > Dashboard*.

You must enable logging for certain features since the information that is compiled for certain Monitor submenus only comes from logs. These features are the UTM Monitor submenus, security policy (Policy Monitor), and the Logging Monitor submenu.

DHCP Monitor

The DHCP Monitor is available from *System > Monitor > DHCP Monitor*. Using this monitor you can view the DHCP servers and relays that are being monitored by the FortiGate unit.

On the DHCP Monitor page, you can also add IP addresses from the page to the IP reservation list. The IP reservation list is a list of reserved IP addresses on a DHCP network for a user who wants to always assign that same IP address to one of the DHCP network's hosts.

On the DHCP Monitor page, you can also refresh the information to ensure current information displays on the page.

Modem Monitor

The Modem monitor is available from *System > Monitor > Modem Monitor*. Using this monitor, you can view the unit's modem status and activity. The information on the page is displayed in a bar chart as well as in a table, located below the bar chart.

On the Modem Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

Session Monitor

The Session Monitor is available from *Policy > Monitor > Session Monitor*. Using this monitor you can view all of the sessions that are currently being monitored by the FortiGate unit. On the Session Monitor page, you can filter the information, delete a session, or refresh the list.

This monitoring submenu is similar to the widget, Top Sessions, which is still available in *System > Dashboard*. The session information that displays in the widget can also be seen within the Session Monitor submenu.

On the Session Monitor page, you can refresh the information to ensure current information displays on the page. You can also filter the information using Filter Settings. If you want to delete a session, select the Delete icon in the row of the session you want removed.

Policy Monitor

The Policy Monitor submenu is available from *Policy > Monitor > Policy Monitor*. Using this monitor you to view the top security policy usage by the FortiGate unit. The information displays in a bar chart and details such as action and packets, are displayed in a table below the bar chart.

On the Policy Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

Load Balance Monitor

The Load Balance Monitor is available from *Firewall Objects > Monitor > Load Balance Monitor*. this monitor display the status of each virtual server and real server, as well as the start or stop status of the real servers, is displayed on the Load Balance Monitor page.

Traffic Shaper Monitor

The Traffic Shaper Monitor is available from *Firewall Objects > Monitor > Traffic Shaper Monitor*. Using this monitor you can view traffic shaping activity that is being monitored by the FortiGate unit. This information displays in a bar chart. You can view the traffic shaper usage information by current bandwidth or by dropped packets. Use the *Report By* drop-down list on the page to view traffic shaper usage by selecting either *Current Bandwidth* or *Dropped packets*.

On the Traffic Shaper Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

AV Monitor

The AV Monitor is available from *UTM Profiles > Monitor > AV Monitor*. Using this monitor you can view activity concerning viruses detected by the FortiGate unit. This information displays on the AV Monitor page in a bar chart as well as in a table located below the bar chart.

On the AV Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

Intrusion Monitor

The Intrusion Monitor is available from *UTM Profiles > Monitor > Intrusion Monitor*. Using this monitor you can view the attack activity detected by the FortiGate unit. This information displays on the Intrusion Monitor page, in a bar chart as well as in a table located below the bar chart.

On the Intrusion Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

Web Monitor

The Web Monitor is available from *UTM Profiles > Monitor > Web Monitor*. Using this monitor you can view the web activity detected by the FortiGate unit. This information displays on the Web Monitor page, in a pie chart and bar chart. The total HTTP requests information displays in the pie chart and the blocked HTTP requests display in a bar chart. The total number of web requests display at the bottom of the charts, in *Total Web Requests (HTTP): <number>*.

On the Web Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

Email Monitor

The Email Monitor is available from *UTM Profiles > Monitor > Email Monitor*. Using this monitor you can view the email activity detected by the FortiGate unit. This information displays on the Email Monitor page, similar to how the Web Monitor page displays its monitoring information, the total number of emails in a pie chart and the blocked emails in a bar chart. The total number of emails is located at the bottom of the charts, in *Total Emails: <number>*.

On the Email Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

Archive & Data Leak Monitor

The Archive & Data Leak Monitor is available from *UTM Profiles > Monitor > Archive & Data Leak Monitor*. Using this monitor you can view the DLP usage performed that is being detected by the FortiGate unit. This information displays in a bar chart. You can view this information by security policy, DLP sensor, or by protocol using the *Report By* drop-down list. The total number of dropped DLP archives is located at the bottom of the chart, in *Total Dropped Archives: <number>*.

On the Archive & Data Leak Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

Application Monitor

The Application Monitor is available from *UTM Profiles > Monitor > Application Monitor*. Using this monitor you can view the application usage detected by the FortiGate unit. This information displays in a bar chart.

On the Application Monitor page, you can refresh the information to ensure current information displays on the page. You can also reset the information, which removes the information from the page and starts the monitoring process again.

IPsec Monitor

The IPsec Monitor is available from *VPN > Monitor > IPsec Monitor*. Using this monitor you can view the activity on IPsec VPN tunnels. The page also shows the start and stop of tunnel activity.

The list includes both dial-up IPsec users as well as static IP or Dynamic DNS VPNs. The list provides status and IP addressing information about VPN tunnels, which VPN tunnels are active or non-active, connecting to remote peers that have static IP addresses or domain names. If you want, you can also start and stop individual tunnels from the list as well.

SSL-VPN Monitor

The SSL Monitor is available from *VPN > Monitor > SSL-VPN Monitor*. Using this monitor you can view the activity of SSL VPN sessions. The list displays the user name of the remote user, the IP address of the remote client, and the time the connection was made. You can also see which services are being provided, and delete an active web or tunnel session from the unit.

Web Cache Monitor

The Web Cache Monitor is available from *WAN Opt. & Cache > Monitor > Cache Monitor*. Using this monitor you can view the activity of SSL VPN sessions. The web cache monitor includes two widgets that display information about web cache requests and web cache traffic. The Web Cache Requests widget displays the number of session that were cached and the number that were not in a pie chart. The Web Cache Traffic widget consists of a line graph that compares the amount of HTTP traffic in kbytes on the WAN with the amount of HTTP traffic in kbytes on the LAN. The difference between the LAN and WAN traffic shows how much traffic was cached.

WAN optimization Peer Monitor

The WAN optimization Peer Monitor is available from *WAN Opt. & Cache > Monitor > Peer Monitor*. Using this monitor you can view a list of WAN optimization peers that the FortiGate unit can communicate with. For each peer you can view the peer's name and IP address, the type of peer, and the amount of traffic reduction as a result of WAN optimization or web caching with that peer.

WAN optimization web cache monitor

To view the web cache monitor, go to *WAN Opt. & Cache > Monitor > Cache Monitor*.

The web cache monitor shows the percentage of web cache requests that retrieved content from the cache (hits) and the percentage that did not receive content from the cache (misses). A higher the number of hits usually indicates that the web cache is being more effective at reducing WAN traffic. To improve cache performance you can

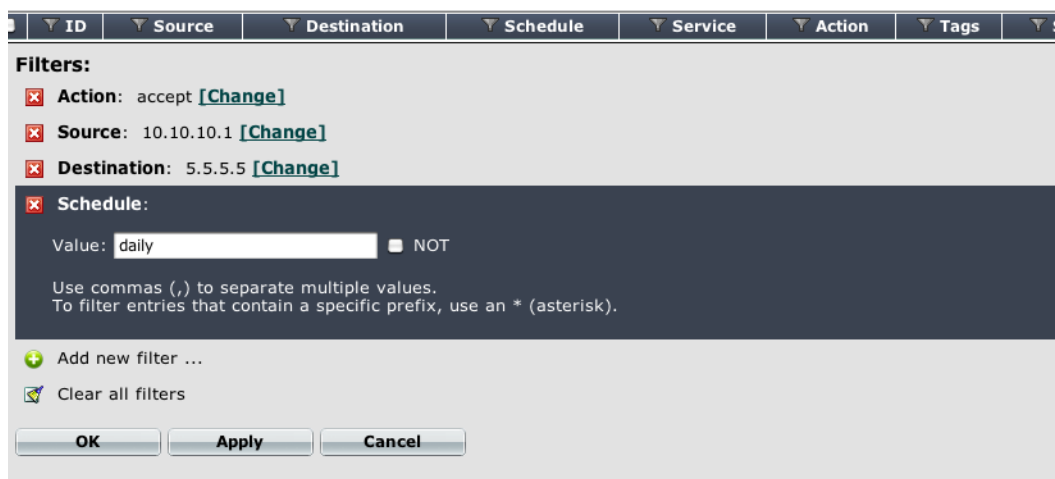
The web cache monitor also shows a graph of web traffic on the WAN and LAN. A lower WAN line on the graph indicates the web cache is reducing traffic on the WAN. The web cache monitor also displays the total number of web requests processed by the web cache.

Filtering web-based manager lists

In previous releases, when you wanted to filter information within a web-based manager list you used the filter icons. Filter icons are still available for filtering, however, *Filter Settings* have been introduced, providing a central location to configure multiple filters at once. Previously, you had to configure filters one at a time.

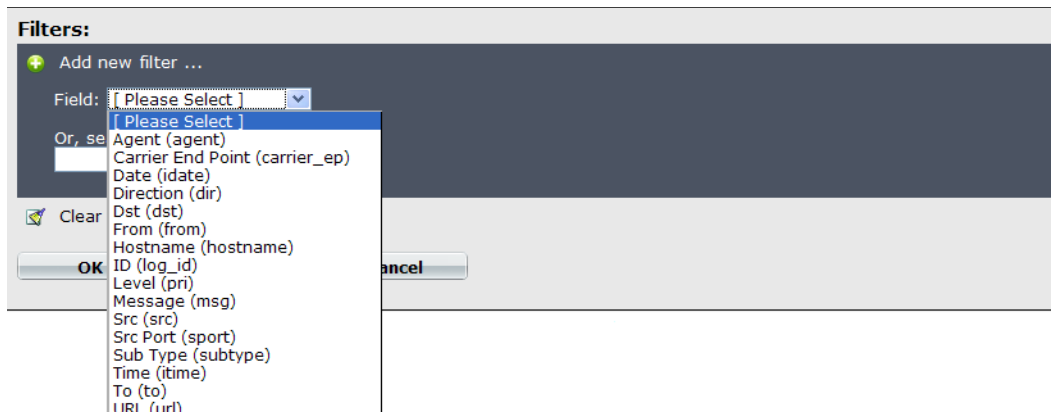
When you select *Filter Settings*, a new *Filters:* pane appears at the top of the list. You can use this pane to add and remove multiple filters and configure settings for each one. Add a filter by selecting Add new filter or by selecting the filter icon for a column in the list. When you select a filter icon in a list column the Filters pane opens with that column added to it.

Figure 10: Filter Settings



You must select *OK* when you are ready to apply the filters, otherwise the filter settings will not be applied to the information on the page. You can modify or remove a filter at any time.

Figure 11: Example of adding a log field from the Field drop-down list when filtering log messages



Reference count column (object usage visibility)

Within most web-based manager lists, a new column displays called the Reference count column, or *Ref.* This new column shows that a configuration object (for example an interface) is referenced to another object (for example a security policy) and how many times that object is referenced within FortiOS. For example, in [Figure 12](#) the default antivirus profile is referenced once. Finding a referenced object in previous releases was available only in the CLI.

Figure 12: The Ref. count column in the firewall address list

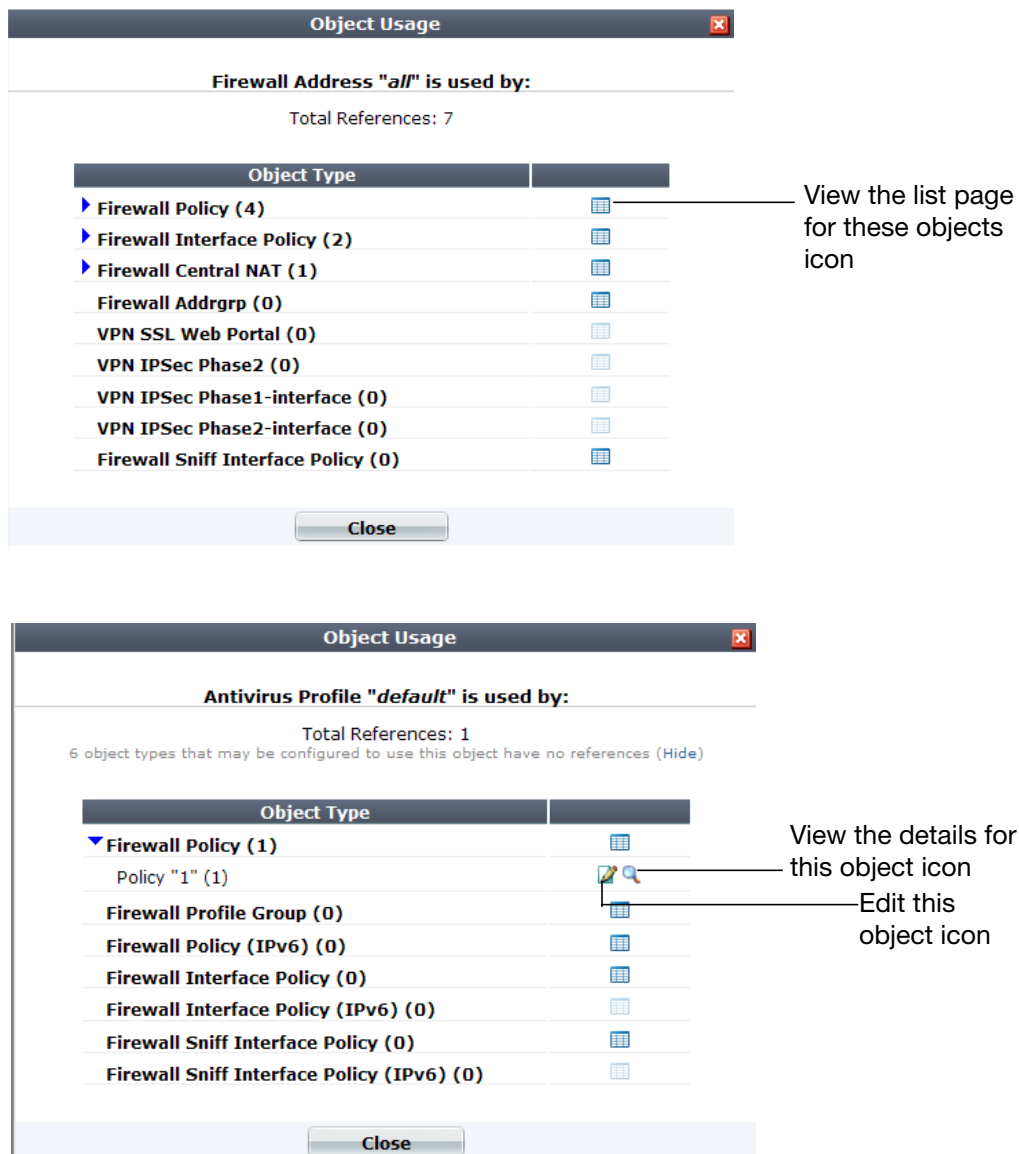
	Name	Address/FQDN	Interface	Type	Ref.
<input type="checkbox"/>	all	0.0.0.0/0.0.0.0	Any	Subnet	10
<input type="checkbox"/>	SSLVPN_TUNNEL_ADDR1	10.0.0.[1-10]	Any	IP Range	2
<input type="checkbox"/>	all	::/0		IPv6	0

The *Ref.* column helps you to determine the object that is being referenced, and where it is referenced in. The *Ref.* column also helps you when you need to remove an object but are unable to because it is being referenced.

When you select the number within the reference count column, the Object Usage window appears, showing you exactly where the object is referenced within an object type. An object type in this usage is the location of where an object is referenced in. For example, in [Figure 13](#) the Object Usage window shows that the firewall address “all” is referenced within seven object types; in the default antivirus profile, it is referenced once in a security policy.

By selecting on the *View the list page for these objects* icon, you are automatically redirected to the page where the entry is referenced in. When you see the Expand Arrow beside some of the object types, it means that you can either view the location of the object in that particular object type, or modify the object type.


Figure 13: Two views of the Object Usage window, one without any expanded object types, and one with an object type expanded showing the available icons



The Object Usage window also provides a way to view the settings for an object, as seen in Figure 1.

Table 1: The Object Usage window displaying the object type table

Object Usage	
Firewall Address	
Total Refer	
Object Type	
policyid	1
status	enable
orig-port	5
nat-port	12-20

 If you have selected *View the list page for these objects*, and are on the page where the entry is referenced, you can go back to the previous location by selecting the back option on your browser.

Configuration object tagging and coloring

The Tag Management menu provides a central location to view, search and manage tags that you created. Tags are keywords or a term that is assigned to a specific configuration that can be used for searching or filtering purposes.

From this central location in *System > Config > Tag Management*, you can do any of the following:

- a search to find a specific tag
- view where a tag is referenced, for example, a single tag could be referenced in a security policy, predefined signature and application
- go to where the tag is located, for example, a security policy
- view how many tags are currently unused
- remove tags.

The Tag Management page also provides a way to easily locate a specific object, such as a security policy, because of how tags work. For example, an SSL VPN security policy is tagged with the keywords `ssl vpn`, `SSL VPN`, `remote`, and `ssl branch office`; from the Tag Management page, enter `ssl` and the tags for that security policy appear; select one of the tags and within the Object Usage window, select to go to the SSL VPN security policy.

You can view detailed information about what object is using a tag by selecting one of the tags in the rectangular area that contains a gray background. The Object Usage window appears, which displays similar information as when you select a number in the *Ref.* column.

Figure 14: Tag Management page with the option to remove four unused tags




Adding tags to configuration objects

Tags can be created for security policies and firewall addresses. Tags are keywords or a term that is assigned to a specific piece of information, for example a firewall address, which can then be used for filtering or searching purposes.

Tags created within security policies and firewall addresses are used only for filtering and searching purposes. This provides a more concise output. For example, you have multiple VDOMs that contain multiple security policies; tags applied to these security policies allow you to find specific security policies within specific VDOMs.

Tags can also be added to predefined signatures and applications and are used within IPS and application sensors so that only those signatures are used.

The following example explains how to add tags to multiple security policies and then use Tag Management to find a security policy using the tags that were applied to the security policy. Tags are used in the same way for firewall addresses so the example can also be used as basis when configuring and applying tags for firewall addresses.



In the Add Tags window, you can select to add existing tags to the security policy or address list; however, these tags belong to predefined signatures and applications as well as to other security policies and address lists so the tags may not be applicable. You should make sure that the tag is valid for its use when applied to a security policy or other object otherwise it becomes redundant.

Example of how to find a security policy using Tag Management

Your FortiGate unit contains many security policies and the unit is currently in VDOM mode. You want to apply tags to only the SSL VPN security policies so that you can easily get to those policies. There are two SSL VPN security policies.

To add tags to multiple security policies

- 1 In vdom_1, go to *Policy > Policy > Policy*.
- 2 For the first security policy, select it in the row to highlight it.
- 3 Select the down arrow beside *Edit*, and then select *Add Tags*.
- 4 In the Add Tags window, enter `remote ssl, ssl vpn, remote, intranet, non-public, internal` and then select the plus sign.
By selecting the plus sign, the tag is automatically added. If you do not select the plus sign, the tag is not added and you have to enter the tag again.
- 5 Select *OK*.
- 6 In the second security policy, select it in the row to highlight it.
- 7 Select the down arrow beside *Edit*, and then select *Add Tags*.
- 8 In the Add Tags window, enter `internet, ssl vpn, remote, public, external` and then select the plus sign.
- 9 Select *OK*.

To search for a security policy from Tag Management

- 1 Go to *System > Config > Tag Management*.
- 2 On the Tag Management page, enter `remote` in the *Type to find tags: search* field.
The tag appears in the rectangular box with the gray background.
- 3 Select `remote` to view where the tag is currently being used.
- 4 In the Object Usage window, select the *View the list page for these objects* icon in the row of the *Object Type*.
You are redirected to the *Policy > Policy > Policy*, where you can select the security policy and then make changes to that policy.

Adding tags to predefined signatures and applications

Tags can be created for predefined signatures and applications which are then used in a sensor to provide a means to specify the use of only those tagged objects. Tags are keywords or a term that describes a piece of information and are assigned to that specific piece of information.

Tags that are created within a signature in *UTM Profiles > Intrusion Protection > Predefined* can be used within an IPS sensor by applying that same tag in an IPS filter entry. Tags that are created are not displayed within the IPS filter list; you must view them from within the IPS filter itself.

Tags that are created within an application in *UTM Profiles > Application Control > Application List* are applied to an application entry within an application sensor. Tags are used in the exact same as they are for IPS sensors. Tags that are used for predefined signatures cannot be used for applications within the application control list and vice versa.

Tags can also be added to security policies and address lists. When you want to view all tags that are configured for predefined signatures, application control list, security policies and addresses, go to *System > Config > Tag Management*.



















Security configuration object icons

Within the Firewall Objects menu, there are now firewall configuration object icons that you can change the color for. For example, within *Firewall Objects > Address > Address*, the configuration object icon for IP/Netmask was changed to pink.

These icons also include representing an action within the Action column in security policies. For example, for a deny security policy the Action column on the IPv6 Policy page shows a red circle with a line through it.

The following table explains the security policy configuration object icons that you can customize the color for.

Table 2: Security policy configuration object icons

Icon	Definition	Icon	Definition
	Allow		Recurring schedule
	Deny		One-time schedule
	IPsec		Schedule group
	SSL VPN		Pre-defined service
	IP/Netmask		Custom Service
	IP Range		Service Group
	IPv6 Address		Virtual IP
	FQDN Address		Virtual Server
	Address group		Virtual IP Group

Access to online help

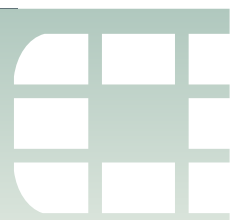
Online help is stored and accessed from our Tech Docs web site; previously it was within the firmware image itself. Online help works in the exact same way as before, providing the same search capabilities as well.

Backing up and restoring configuration files per-VDOM

From the Global VDOM, you can now back up or restore a configuration file for a specific VDOM within the web-based manager. This provides a quick and easy way to back up or restore your configuration file within a specific VDOM. There is an option to back up or restore the full configuration, if needed.

You can back up or restore a specific VDOM configuration file from the System Information widget. When you are on the Backup or Restore page, the *VDOM Config* option is available and you can then choose the specific VDOM you want to back up or restore the configuration from by selecting a VDOM from the drop-down list. These options are only available when you are in the Global VDOM.

This feature is available only when VDOMs are enabled on the FortiGate unit.



More New Features

This section describes additional new features available in FortiOS 4.0 MR3 and contains the following sections:

- New features for FortiOS 4.0 MR3 Patch 7
- New features for FortiOS 4.0 MR3 Patch 6
- New features for FortiOS 4.0 MR3 Patch 5
- New features for FortiOS 4.0 MR3 Patch 4
- New features for FortiOS 4.0 MR3 Patch 3
- New features for FortiOS 4.0 MR3 Patch 2
- New features for FortiOS 4.0 MR3 Patch 1
- Login grace timer for SSH connections
- FortiManager automatic authorization
- Dynamic DNS commands
- New diagnose commands
- New get commands
- MTU configuration support on non-IPsec tunnel interfaces
- Customizing maximum number of invalid firewall authentication attempts
- Controlling the connection between a FortiManager unit and a FortiGate unit
- Bringing up or down IPsec tunnels
- Configuring active CPUs
- Formatting multiple disk partitions
- Transparent mode port pairs
- DNS server changes
- DHCP Server changes
- Installing firmware on a partition without a reboot
- SNMP enhancements
- Replacement message changes
- VDOM and global privileges for access profiles
- HA dynamic weighted load balancing
- VRRP virtual MAC address support
- FGCP HA subsecond failover
- Static Route enhancements
- Monitoring ISIS from the Routing Monitor page
- Security Policy and Firewall Object Enhancements
- Virtual IP source address filter support
- Virtual IP port forwarding enhancements

- Load balancing HTTP host connections
- Web Proxy Service and Web Proxy Service Group
- SSL renegotiation for SSL offloading provides allow/deny client renegotiation
- SSL VPN Port forwarding support
- IKE negotiation
- SHA-384 and SHA-512 support for IKE
- FortiOS Carrier URL extraction feature

New features for FortiOS 4.0 MR3 Patch 7

- The VDOM limit for the FortiGate 1000C and FortiGate 1240B models increased from 100 to 250
- Logging optimization including disk logging separated from FortiAnalyzer logging and other features. See [“Logging performance optimization for FortiOS 4.0 MR3 patch 7” on page 44](#)
- DoS Policies and DoS Sensors removed from the Web-based Manager on low end FortiGate models
- FortiGuard Web Filter Local Ratings and Local Categories have been simplified and are now called Rating Overrides (go to *UTM Profiles > Web Filter > Rating Overrides*)
- Traffic log messages include source country names retrieved from the FortiGuard geographic address database
- FortiGuard Web Filter Quota settings have been enhanced and simplified (go to *UTM Profiles > Web Filter > Profile > FortiGuard Categories > Quota on Categories with Monitor, Warning and Authenticate Actions* and select *Create New* to add a Web Filtering Quota)
- Separate licenses and updates required for IPS Definitions and Vulnerability Scan definitions (go to *System > Config > FortiGuard > IPS & Vulnerability Scan*)
- Increased the SNMP Location Field string length
- For FortiOS Carrier increase the number of GTP profiles to 1000
- Enhanced FortiGuard Analysis and Management Service (FAMS) provides secure reliable cloud-based log message storage, reporting, and analysis. By default, low end models send log messages to FAMS instead of storing them on the FortiGate flash drive or in memory. See [“FortiGuard Analysis and Management Service \(FAMS\)” on page 41](#).
- Log search progress bar

New features for FortiOS 4.0 MR3 Patch 6

See the release notes for a complete list of the enhancements to patch 6.

New features for FortiOS 4.0 MR3 Patch 5

- Intrusion Protection (IPS) is now supported for load balancing virtual servers (load balancing virtual IPs (VIPs)). You can now enable UTM and select an IPS sensor in a firewall policy that contains a load balancing virtual server. This includes the case where the load balancing virtual server supports persistence. However, IPS does not work with virtual server load balancing of SSL sessions.

New features for FortiOS 4.0 MR3 Patch 4

- Combine IPS and vulnerability management service into one section
- Move disk management to *System > Config > Advanced > Disk Management*
- Disable memory logging for low-end models with large flash drives
- Enhance memory logging for low-end models with no log disk
- WAN Opt & Cache no longer available on the web-based manager for low-end FortiGate/FortiWiFi models since these features can affect performance of the low-end models. The features are still available from the CLI.

New features for FortiOS 4.0 MR3 Patch 3

- FortiGuard Web Filter category update
- Multiple email fields in log messages
- Weekly Report in PDF and Web Format
- Up to 100 VDOMs supported for the FortiGate-1240B
- [“WAN optimization web cache monitor” on page 64.](#)

New features for FortiOS 4.0 MR3 Patch 2

The following is a list of changes made to FortiOS 4.0 MR3 Patch 2:

- Central Management has been moved from *System > Admin > Central Management* to *System > Admin > Settings*.
- The web-based manager page for adding and editing security policies has been enhanced to make policies easier to configure and understand.
- [“WAN optimization Peer Monitor” on page 64.](#)
- FortiClient Connect is now called FortiClient.
- From *System > Certificates > CA Certificates*, the Fortinet_Wifi_CA certificate is now called PositiveSSL_CA.
- FortiGate-VM now has a 15-day trial evaluation license and upgrade available.
- Firewall address table size has been increased to 2000 on FortiGate-110C, 200A, 200B, and 80C series models.
- Static route entries table size has been increased to 5000 for the FortiGate-310B and 300C models.
- Support for load balancing on the FMG-XG2 card is now available.
- The Session widget now contains offload information in the Offload information column.
- In *Firewall Objects > Service > Service Groups*, the following are default service groups you can use:
 - *Exchange Server*
 - *Exchange Service OWA*
 - *Outlook*
 - *Windows AD*

- In *Firewall Objects > Service > Web Proxy Service*, there is one default web proxy service available for you to use.
- You can now capture packets within the web-based manager by going to *System > Config > Advanced* and creating a packet capture filter. You can start and stop a filter at any time.
- Support is now available for 64bit FortiOS on the FortiGate-1240B.
- When configuring wireless settings in an SSID for wireless networking, you can now choose to have both TKIP and AES.
- On the Application Control Monitor page, it has changed to look similar to a Dashboard page. There are three widgets and each display data using specific commands in the CLI. The three widgets are:
 - Top Applications by Bandwidth (use `diag stats app-bandwidth`)
 - Top Applications by Session Count
 - Top IP/User for `<ip address_application>` (use `diag stats app-usage-ip <address/application>`)
- SQL logging may or may not be, by default, enabled on certain models. You should verify that SQL logging is enabled after upgrading to FortiOS 4.0 MR3 Patch-2.
- Report function may be affected by the change of logging back to text-based logs.
- For FortiGate models that support SSD, the default database size is 10GB in a single VDOM environment. FortiGate models that support a flash drive, their default database size is 1.5GB. You can change this default size to meet your own network logging requirements.
- When searching for information in logs in the web-based manager, you may not be able to continue searching if your search resulted in less than 50 records. Use the CLI instead if you want to continue your search.
- When configuring RADIUS servers for dynamic profile configurations, you can now choose to close all sessions associated with an IP address when a RADIUS STOP message is received. You can also enable logging of these RADIUS message events. A dynamic profile group must be configured first, before these RADIUS configuration settings become available within the New RADIUS Server page.
- Load balance mode allows you increased flexibility in how you use the interfaces on the FortiGate unit. When enabled on a FortiGate-3140B or a FortiGate-3950B/3951B with an installed FMC-XG2, traffic between any two interfaces (excluding management and console) is accelerated. Traffic is not limited to entering and leaving the FortiGate unit in specific interface groupings to benefit from NP4 and SP2 acceleration. You can use any pair of interfaces.

Security acceleration in this mode is limited, however. Only IPS scanning is accelerated in load balance mode.

New features for FortiOS 4.0 MR3 Patch 1

The following is a list of changes made to FortiOS 4.0 MR3 Patch 1.

- The configuration of Web Filtering local ratings and local categories has been simplified.
- Support FSSO and sniffer policies: Log messages recording information gathered by a sniffer policy include a user name if the IP address in the log message corresponds to the IP address if a user who has been authenticated with FSSO.

- Web Filter Profile, IPS and application control pages of the web-based manager have been changed to enhance usability.
- [“High-level web-based manager menu changes” on page 57.](#)
- FortiGate unit Central Management Locking: FortiGate configuration changes cannot be made of the CLI or web-based manager if the unit is being remotely managed from FortiManager.
- FortiOS 4.0 MR3 patch 1 is compatible with FortiClient. FortiGate units support up to 10 FortiClient Connect connections.
- The new FortiGate UTM Weekly Activity Report now includes support for data based on geographic locations. For example, the default report includes a graph of Top Destination Countries by session
- BGP dynamic routing now supports AS override. With `as-override` enabled, while advertising an AS path to a peer, all leading occurrences of the peer's AS number are replaced with the AS number of the advertising router.

```
config router bgp
  config neighbor
    edit 192.168.1.112
      ...
      set as-override disable|enable
      set as-override6 disable|enable
      ...
```

- Forward and reverse traffic shaping can now be set independently in security policies and in application control sensors
- The WiFi controller feature in a FortiWiFi unit can manage local WiFi functions in the same manner as a remote FortiAP or FortiWiFi unit.
- SMTP virus scanning now supports scanning of STARTTLS messages.
- [“Web Cache Monitor” on page 64.](#)
- Control whether to bypass or block SSL sessions that cannot be decrypted by SSL content scanning and inspection. This behavior is controlled from the CLI in a protocol options profile. For example, for POP3S:

```
config firewall profile-protocol-options
  edit new_profile
    config pop3s
      set unsupported-ssl {bypass | block}
      ...
```

- When adding LDAP, RADIUS or TACAS+ authentication servers you can select Test to verify that the configuration is correct. You can also use `diagnose test authserver` commands to test a number of aspects of authentication server configuration.
- LDAP group checking is now supported using the following command. You can set LDAP group checking to perform group object checking or user attribute checking.

```
config user ldap
  edit new_ldap
    set group-member-check {group-object | user-attr}
    set unsupported-ssl {bypass | block}
```

- FortiOS Carrier supports GTPv1 release 7.15.0 and GTPv1 release 8.12.0

Login grace timer for SSH connections

A grace timer has been introduced which allows control over the login time limits of SSH connections to the FortiGate unit. The grace timer can close open but unauthenticated SSH connections to the FortiGate unit. For example, if the timer is set to 60 seconds, any open, unauthenticated SSH session is closed after 60 seconds.

The default value of the allowed time is 120 seconds but can be configured for 10 to 3600 seconds.

This feature is available only in the CLI. The CLI command syntax used is:

```
config system global
  set admin-ssh-grace-time <seconds>
end
```

FortiManager automatic authorization

In previous releases, the `authorize-manager-only` command restricted access to authorized FortiManager units. This authorization is now automatically found during the communication exchanges between the FortiGate and FortiManager units.

This automatic authorization behaves as follows:

- On the FortiManager unit, an administrator enters the management IP or FQDN of the FortiManager unit.
- During the protocol exchange between the two units, on the FortiManager unit's side that management IP or FQDN is sent to the FortiGate unit.
- The FortiGate unit, after receiving the management IP or FQDN, determines that is valid, saves that management IP or FQDN as the FortiManager unit's

Dynamic DNS commands

The following DDNS commands were removed from the `config system` interface command. The DDNS commands are now found under the new `config system ddns` command.

```
set ddns {enable | disable}
set ddns-server <server>
set ddns-domain <server>
set ddns-username <username>
set ddns-password <password>
```

The DDNS commands above now in the `config system ddns` command:

```
set monitor-interface <interface_name>
set ddns-server <server>
set ddns-domain <domain_name>
set ddns-username <username>
set ddns-password <password>
```

New diagnose commands

Real-time session, traffic shaper bandwidth and CP6 statistics

The following CLI commands display real-time session set up rate statistics, accurate current traffic shaper bandwidth, and CP6 statistics information.

```
diag hardware ipsec
diag hardware deviceinfo cp6 {brief | cmdq | cmdqdis | rng |
task}
```

The CLI command `diag firewall shaper traffic-shaper list` now displays the accurate current traffic shaper bandwidth.

diag sys session filter proto-state

A new `diag` command has been introduced, which is an enhancement to the `get sys session-info {stat|full-stat}` command. The new command includes counts of the various TCP states, which the `get sys session-info stat|full-stat` command previously did not have.

The `diag sys session filter proto-state` command allows you to view the counts of various TCP states. This command can help in enterprise-type environments when tuning various protocol timers, for example, there are 60 percent of sessions in syn-sent state in comparison to the established sessions.

diag log-stats show

The new `diag log-stats show` command displays the number log messages that were discarded by the unit.

New get commands

IPsec get commands

There are several new `get` commands that help you to view IPsec VPN tunnel information as well as IKE gateway information and IPsec tunnel statistics.

The following `get` commands for IPsec VPN are as follows:

```
get vpn ike gateway
get vpn ipsec stats crypto
get vpn ipsec stats tunnel
get vpn ipsec tunnel summary
get vpn ipsec tunnel details
get vpn ipsec tunnel name
```

An example of the output of the `get vpn ipsec tunnel summary` is:

```
gateway
  name: 'phase1'
  type: policy-based
  local-gateway: 0.0.0.0:0 (dynamic)
  remote-gateway: 10.10.5.24:0 (static)
  mode: ike-v1
  interface: 'wan2' (4)
  rx packets: 0 bytes: 0 errors: 0
  tx packets: 0 bytes: 0 errors: 0
  dpd: enabled/unnegotiated
  selectors
    name: 'phase2'
    auto-negotiate: disable
    mode: tunnel
    src: 0:0.0.0.0/0.0.0.0:0
    dst: 0:0.0.0.0/0.0.0.0:0
```

The `get vpn ipsec stats tunnel` command gives statistics about the total number of IPsec tunnels and their types, including the number of selectors, how many are up, and any errors.

The following `get` commands for IPsec are now removed:

```
get vpn status concentrators
get vpn status ike config
get vpn status ike errors
get vpn status ike routers
get vpn status ike status detailed
get vpn status ike status summary
get vpn status ipsec
get vpn status tunnel stat
get vpn status tunnel dialup-list
get vpn status tunnel number
```

The following commands were changed:

- `get vpn status ike gateway` is replaced by `get vpn ike gateway`
- `get vpn status tunnel list` is replaced by `get vpn ipsec tunnel summary` and `get vpn ipsec tunnel details`
- `get vpn status tunnel name` is replaced by `get vpn ipsec tunnel name`
- `get vpn status ike crypto` is replaced by `get vpn ipsec stats crypto`

Traffic shaper and per-IP shaper

You can now view traffic shaper and per-IP shaper information from within the CLI. The commands display general information about shapers which includes their current bandwidth.

These commands are within the `get` command branch:

```
get firewall shaper traffic
get firewall shaper per-ip-shaper
```

Management checksum configuration information for FortiManager

There are now three new `get` commands that allow you to view the configuration checksum information to the FortiManager unit.

The management checksum commands are:

```
get system mgmt-csum global
get system mgmt-csum vdom <vdom_name>
get system mgmt-csum all
```

If you have no VDOMs enabled, entering `get system mgmt-csum` allows you to view the overall checksum information. The following is an example:

```
get system mgmt-csum
debugzone
global: 5c d6 08 fd e5 52 b3 18 e3 4d be 7f dc 40 86 66
root: 04 02 f0 e5 f2 21 36 63 72 05 f5 dc 31 94 c5 63
all: 24 90 19 d0 e4 67 7a c1 81 99 67 ae 77 fa bb 01

checksum
global:5c d6 08 fd e5 52 b3 18 e3 4d be 7f dc 40 86 66
root: 04 02 f0 e5 f2 21 36 63 72 05 f5 dc 31 94 c5 63
all: 24 90 19 d0 e4 67 7a c1 81 99 67 ae 77 fa bb 01
```


MTU configuration support on non-IPsec tunnel interfaces

MTU configuration for non-IPsec tunnel interfaces is now supported. This allows you to customize the transmission amount for each interface on the FortiGate unit.

MTU is configured only in the CLI. The MTU setting is hidden until you enable the `mtu-override` setting.

Customizing maximum number of invalid firewall authentication attempts

A new option in the `config user setting` command allows you to customize the maximum number of invalid firewall authentication attempts before the FortiGate unit blocks them. This provides a way to tune CPU usage against invalid authentication connections.

The new option in the `config user setting` command is `auth-invalid-max`, and you can set the value between 1 and 100. For example, entering five allows five invalid authentication attempts before the unit blocks the user.

The following is an example of using this feature.

```
config user setting
  set auth-invalid-max 3
end
```

Controlling the connection between a FortiManager unit and a FortiGate unit

In the `config system interface` command, you can now configure whether an interface lets a FortiManager unit connect with a FortiGate on that unit's interface. For example, port 2 on the FortiGate unit does not allow the FortiManager unit to connect to it. When the FortiManager unit tries to connect to the FortiGate unit, the FortiGate unit refuses the connection.

If this feature is configured to not allow the FortiGate unit to connect to a FortiManager unit, the FortiGate unit will not allow an administrator to input the FortiManager unit's serial number into the central management configuration.

The command syntax for configuring this feature is as follows:

```
config system interface
  edit <interface>
    set allowaccess {ping | http | https | ssh | telnet | snmp |
fgfm}
  end
```

Bringing up or down IPsec tunnels

Previously, you could activate or shut down IPsec tunnels using the `diag vpn tunnel {up | down}` commands. You can now use the following `execute` commands to help you bring up or down, and IPsec tunnel.

```
execute vpn ipsec tunnel down <phase2> <phase1> <serial>
execute vpn ipsec tunnel up <phase2> <phase1> <serial>
```

When using these `execute` commands, you can optionally use the phase 1 name, phase 2 or serial number to shut down or bring up the tunnel. However, if you are bringing down a tunnel, and that is a dial-up tunnel, phase 1 name is required. Bringing up a tunnel using the `execute vpn ipsec tunnel up` command cannot be used to activate a dial-up tunnel.

Configuring active CPUs

The new global command, `num-cpus`, allows you to configure a set number of active CPUs. This new feature is available only on platforms with eight or more CPUs.

The following is an example of how to configure five active CPUs.

```
config system global
  set num-cpus 10
end
```

Formatting multiple disk partitions

On a FortiGate unit with multiple disk partitions, you can now format multiple partitions at one time. This provides a quick and easy way to format multiple disk partitions.

Formatting multiple disk partitions uses the `execute disk format` command. The formatting process behaves in the following ways:

- If the formatting requires a reboot because one of the partitions is currently in use, all partitions are formatted before the reboot.
- If no reboot is required and an error occurs in the formatting process, the error is written to the event log.
- If an error occurs in formatting and a reboot is required, the error is logged to the event log.
- RAID (enable or disable) and RAID rebuilds take place before the reboot
- The `execute disk format` command requires that you enter each of the reference numbers of the partitions you want formatted. The reference numbers are found using the `execute disk list` command.

Table 3: Explanation of the encryption levels available

Encryption level	Explanation of encryption level	Algorithm associated with encryption level
High	Encryptions with key lengths larger than 128 bits, and some Cipher suites with 128-bit keys.	DHE-RSA-AES256-SHA AES256-SHA EDH-RSA-DES-CBC3-SHA DES-CBC3-SHA DES-CBC3-MD5 DHE-RSA-AES128-SHA AES128-SHA
Medium	Encryptions that are using 128 bit encryption	RC4-SHA RC4-MD5 RC4-MD

Table 3: Explanation of the encryption levels available

Low	Encryptions using 64 or 56 bit encryption but excluding export Cipher suites.	EDH-RSA-DES-CDBC-SHA DES-CBC-SHA DES-CBC-MD5
------------	---	--

Transparent mode port pairs

Port pairing is an option in transparent mode to bind two ports together. In doing this, you can create security policies that regulate traffic only between two specific ports, VLANs or VDOMs. In its simplest form, this enables an administrator to create security policies that are only between these two ports. Traffic is captured between these ports. No other traffic can enter or leave a port pairing.

For example, a FortiGate unit has three ports, where port 1 and port 2 are paired together, because the two networks only need to communicate with each other. If packet arrives on port 1, the FortiGate unit needs to figure out whether the packet goes to port 2 or port 3. With port pairing configured, it is more simple. If packet arrives on port 1, then the FortiGate automatically directs the packet to port 2. The opposite is also true in the other direction. This can be ideal when to groups only need to transfer data between each other.

To configure port pairing - web-based manager

- 1 Go to System > Network > Interface.
- 2 Select the arrow next to the Create New button and select Port Pair.
- 3 Enter a Name for the port pair.
- 4 Select the physical or virtual ports from the Available Members list and select the right-facing arrow to add the ports to the Selected Members.
There can be only two ports added.
- 5 Select OK.

To configure port pairing - CLI

```
config system port-pair
  edit <pair_name>
    set member <port_names>
  end
```

When configuring security policies with the port pairs, selecting the Source Interface automatically populates the Destination Interface, and vice versa. All other aspects of the security policy configuration remain the same.

DNS server changes

Previously, when a DNS request was locally matched to a defined zone with no answer defined, it was not recursively forwarded. In this release, the DNS request is now forwarded when it cannot find a local answer in a non-authoritative zone, provided that the ingress interface has recursive DNS query enabled, using the authoritative option. This option is available within a DNS zone, in *System > Network > DNS Server*.

This new option, *Authoritative*, controls the DNS server's behavior so that it is more flexible. You can enable or disable this option in the web-based manager or CLI.



Fortinet recommends not using a FortiGate unit as an authoritative domain server.

DHCP Server changes

The DHCP Server information in the web-based manager is now located within the Network menu, *System > Network > DHCP Server*. The Network menu also contains the DHCP feature IP Reservation which is located in *System > Network > IP Reservation*. IP Reservation allows you to reserve an IP address that is on a DHCP network for a user who wants to always assign that same IP address to one of the DHCP network's hosts. The DHCP feature also includes support for IPv6.

When you create a new DHCP server, you can configure additional options under the Advanced section of the service page. There can be up to three options configured for a service. You can also add excluded ranges when configuring a DHCP server.

DHCP IP Reservation

Within the DHCP pool of addresses, you can ensure certain computers will always have the same address. This can be to ensure certain users always have an IP address when connecting to the network, or if you want a device that connects occasionally to have the same address for monitoring its activity or use.

In the example below, the IP address 172.20.19.69 will be matched to MAC address 00:1f:5c:b8:03:57.

- 1 Go to *System > Network > DHCP Server*.
- 2 Select the DHCP server from the list or add a new DHCP server.
- 3 Select IP Reservation and select Create New.
- 4 Enter an IP address of 172.20.19.69
- 5 Enter the MAC address of 00:1f:5c:b8:03:57.
- 6 Select OK.

You can also select *Add from DHCP Client List* and select the MAC and IP address pairs to add.

Installing firmware on a partition without a reboot

When you are upgrading the firmware on your FortiGate unit, you now have the option of installing the firmware on a partition without having to reboot the unit and run the image as the active firmware that is running on the unit. You can easily upgrade or downgrade to the firmware of your choice by using this new feature.

The following is an example of how to install the firmware image on a partition and not have the firmware running as the active firmware on the unit. The following also explains how to install the new firmware from the non-active partition and then make it the current active firmware running on the unit.

Example of installing a firmware on a partition without rebooting

You have decided to install FortiOS 4.0 MR3 release on the unit but still want to be able to easily switch back to a FortiOS 4.0 MR2 Patch release afterwards. You currently have two partitions on the unit's local hard disk and would like to be able to switch between the two firmware images at any given time.

The following procedures do not include backing up the configuration file since it is assumed that the back up has already been done.

To install a firmware image on a partition without a reboot

- 1 Go to *System > Dashboard > Status* and locate the System Information widget.
- 2 In the System Information widget, select *Update* in the *Firmware Version* row.
- 3 On the Firmware Upgrade/Downgrade page, select *Local Hard Disk* from the drop-down list beside *Upgrade From*.
- 4 Select *Browse* beside the *Upgrade File* field to locate the firmware image.
- 5 Clear the check box beside *Boot the New Firmware*.

This disables the reboot process that occurs when a firmware is being installed on the FortiGate unit.

- 6 Select *OK*.

A message similar to the following appears:

```
Software upload has completed. To use the new firmware, please
select it under System > Maintenance > Firmware, and use the
'Upgrade' option.
```

- 7 Go to *System > Maintenance > Firmware*.

In the table on the Firmware page, you can see that Partition 1 has the firmware image FortiOS 4.0 MR3 release.

The following procedure assumes that you are already in *System > Maintenance > Firmware*.

To install the new firmware from the partition

- 1 On the Firmware page, select the check box in the row of the firmware image FortiOS 4.0 MR3.
- 2 Select the Upgrade icon, located above the table.

The following message appears:

```
The page at http://172.16.177.153 says:
```

```
System will reboot immediately and the current non-active
partition will be set as the default boot partition. Continue?
```

- 3 Select *OK*.

The Boot alternate firmware page appears with the following message:

```
Please wait for system reboot to the new partition. Refresh your
browser after a few minutes.
```

The unit reboots with the FortiOS 4.0 MR3 as the firmware image actively running on the unit.

SNMP enhancements

The SNMP feature contains several enhancements, as well as changes to the SNMP menu in the web-based manager.

Previously, for SNMP OIDs in FortiOS 4.0, the FortiOS OIDs were re-numbered so that each separate Fortinet product has its own root in the FortiOS OID space. SNMP 3.0 OIDs were still supported in FortiOS 4.0; however, both types of OIDs appear during an SNMP walk. In FortiOS 4.0 MR3 release, they are no longer supported so that only 4.0 SNMP OIDs appear.



IPv6 is now supported for SNMP.

WAN optimization, Web Cache and Explicit proxy MIBs

There are new MIBs for the new web proxy and caching features as well as explicit proxy. Some MIBs are supported by transparent proxy and these can be ported to the explicit proxy. There are also special OIDs for specific models.

SNMPv3

SNMPv3 is now supported. Within the SNMP configuration settings, you can configure SNMPv3 users, and include the events as well. The SNMP menu (*System > Config > SNMP*) provides all the configuration settings to create multiple SNMPv3 users. Each user can have multiple events enabled for them, as well as their specific security level. Multiple notification hosts can also be configured for each user.

SNMPv3 is usually included for additional security and remote configuration enhancements to SNMP. SNMPv3 provides confidentiality, integrity and authentication. For additional information about SNMPv3, see RFC 3411-3418.

Replacement message changes

There are several changes to replacement messages, as well as a new feature that allows you to upload images and use them in certain replacement messages. In this document, uploading images and using them in replacement messages is referred to as image embedding.

Replacement messages that contain authentication pages are now updated using the color scheme and image embedding feature. The types of replacement messages that are updated to the new color scheme and image embedding are:

- disclaimer pages
- login pages
- declined disclaimer pages
- login failed page
- login challenge page
- keepalive page

Endpoint NAC download portal and recommendation portal replacement messages are also updated to the new color scheme and image embedding feature. HTTP replacement messages are also updated.

Archive replacement messages and FTP proxy replacement message

The archive replacement messages and the FTP proxy replacement message are introduced because of the changes that occurred to the antivirus profile with regards to log archival options, and the new FTP proxy.

The following are the archive replacement messages and the FTP proxy replacement message.

- FTP Explicit-banner (under FTP Proxy)
- Archive block message (under HTTP)

Successful firewall authentication replacement message

The new Success message within the Authentication replacement messages provides a message indicating to the authenticating user that they have successfully authenticated their Telnet session. This replacement message is a text-only message.

Web filtering disclaimer replacement message

The web filtering disclaimer page allows users to bypass an override whenever they try to access a blocked page. The FortiGuard Web Filtering override form replacement message contains information so that the user can override the blocked page by authenticating with their user name and password. This replacement message is available in *System > Config > Replacement Message*, under FortiGuard Web Filtering.

Video chat block replacement message

The video chat block replacement message displays when a video chat has been blocked by the FortiGate unit. This message is available in *System > Config > Replacement Message*, under IM and P2P.

Replacement message images

The Replacement Message Image menu allows you to upload your organization or company's image to include in a replacement message. You can upload GIF, JPEG, TIFF, or PNG files, and give the file a unique name as well. The maximum image size that can be uploaded is 6000 bytes.

There are three default Fortinet images that you can choose from: the logo_fg_guard_wf, logo_fnet and logo_fw_auth. The following is a special tag to indicate that an image from the replacement message image list should be used in the replacement message.

```
<img src=%%IMAGE: <config_image_name>%% size=<btyes> >
```

When you include an image in a replacement message, it is referenced by the FortiGate unit. This reference number is displayed in the reference column of the Replacement Message Image page.

VDOM and global privileges for access profiles

Access profiles can now be configured with a VDOM or global privilege. These two privileges allow the FortiGate administrator access to either a specific VDOM or global access. Global access allows access to all VDOMs and global settings. When an administrator's account contains an access profile with a VDOM privilege, that administrator can access only the VDOM that is specified in their account. For example, admin_1 has the access profile admin_vdom; admin_vdom contains read and write privileges for logging and VDOM access; admin_1's account is associated with vdom_1. The admin_1 accessibility is limited to vdom_1 and the ability to configure only log settings.

Previously, when administrator accounts were configured, the VDOM was specified in the administrator account and access permissions were specified in an admin profile. By using this new access profile privilege, you can apply an access profile to an administrator that is specific for VDOM configuration.

These new access profile privileges are available only in the CLI. A new command, `scope`, provides the ability to have an access profile contain VDOM privileges or global privileges.

Example of incorporating the new access profile to existing administrator accounts

Company_A's branch office requires two administrators to access their FortiGate unit and they currently have VDOMs configured. An administrator with global access must be configured and an administrator with VDOM access that can configure reports are required.

There are currently two administrator accounts that contain global access and VDOM access to the FortiGate unit. However, management wants to apply the new privileges to the existing accounts.

This example explains how to incorporate the new privileges into two existing administrator accounts. The existing administrator accounts are admin_vdom and admin_global. You need to configure a global access profile because you cannot modify the super_admin access profile.

To modify the existing access profiles

- 1 Log in to the CLI and then in to the global level.

```
config global
```

- 2 Enter the following command within the global VDOM:

```
config system accprofile
```

- 3 Modify the vdom access profile first:

```
edit vdom
  set scope vdom
next
```

The admin_vdom account will now be only able to access VDOMs within the configuration.

- 4 Enter the following commands to modify the global access profile:

```
edit global
  set scope global
  set admingrp read-write
  set authgrp read-write
```



```

set endpoint-control-grp read-write
set fwgrp read-write
set loggrp read
set mntgrp read-write
set netgrp read-write
set routegrp read-write
set sysgrp read-write
set updategrp read-write
set utmgrp read-write
set vpngrp read-write
set wanoptgrp read-write
end

```

- 5 Enter the following command to apply the new global access profile to the existing `admin_global` administrator account:

```

config system admin
  edit admin_global
    set accprofile global
end

```

You can verify that the access profiles have their global and VDOM privileges by going to *System > Admin > Administrators* and viewing the *Scope* column. In the *Scope* column, `admin_vdom` contains `VDOM: vdom_1`, and in the `admin_global`.

HA dynamic weighted load balancing

The following explains the weighted failover feature that is supported in this release. It is explained in two parts; the configuration of weighted-round-robin weights and weighted load balancing.

Configuring weighted-round-robin weights

You can configure weighted round-robin load balancing for a cluster and configure the static weights for each of the cluster units according to their priority in the cluster. When you set `schedule` to `weight-round-robin` you can use the `weight` option to set the static weight of each cluster unit. The static weight is set according to the priority of each unit in the cluster. A FortiGate HA cluster can contain up to 16 FortiGate units so you can set up to 16 static weights.

The priority of a cluster unit is determined by its device priority, the number of monitored interfaces that are functioning, its age in the cluster and its serial number. Priorities are used to select a primary unit and to set an order of all of the subordinate units. Thus the priority order of a cluster unit can change depending on configuration settings, link failures and so on. Since weights are also set using this priority order the weights are independent of specific cluster units but do depend on the role of the each unit in the cluster.

You can use the following command to display the priority order of units in a cluster. The following example displays the priority order for a cluster of 5 FortiGate-620B units:

```

get system ha status
Model: 620
Mode: a-p
Group: 0
Debug: 0
ses_pickup: disable
Master:150 head_office_cla FG600B3908600825 0

```

```

Slave :150 head_office_clb FG600B3908600705 1
Slave :150 head_office_clc FG600B3908600702 2
Slave :150 head_office_cld FG600B3908600605 3
Slave :150 head_office_cle FG600B3908600309 4
number of vcluster: 1
vcluster 1: work 169.254.0.1
Master:0 FG600B3908600825
Slave :1 FG600B3908600705
Slave :2 FG600B3908600702
Slave :3 FG600B3908600605
Slave :4 FG600B3908600309

```

The cluster units are listed in priority order starting at the 6th output line. The primary unit always has the highest priority and is listed first followed by the subordinate units in priority order. The last 5 output lines list the cluster units in vcluster 1 and are not always in priority order.

The default static weight for each cluster unit is 40. This means that sessions are distributed evenly among all cluster units. You can use the `set weight` command to change the static weights of cluster units to distribute sessions to cluster units depending on their priority in the cluster. The weight can be between 0 and 255. Increase the weight to increase the number of connections processed by the cluster unit with that priority.

You set the weight for each unit separately. For the example cluster of 5 FortiGate-620B units you can set the weight for each unit as follows:

```

config system ha
  set mode a-a
  set schedule weight-round-robin
  set weight 0 5
  set weight 1 10
  set weight 2 15
  set weight 3 20
  set weight 4 30
end

```

If you enter the `get` command to view the HA configuration the output for `weight` would be:

```
weight 5 10 15 20 30 40 40 40 40 40 40 40 40 40 40
```

This configuration has the following results if the output of the `get system ha status` command is that shown above:

- The first five connections are processed by the primary unit (host name `head_office_cle`, priority 0, weight 5). From the output of the
- The next 10 connections are processed by the first subordinate unit (host name `head_office_clb`, priority 1, weight 10)
- The next 15 connections are processed by the second subordinate unit (host name `head_office_clc`, priority 2, weight 15)
- The next 20 connections are processed by the third subordinate unit (host name `head_office_cld`, priority 3, weight 20)
- The next 30 connections are processed by the fourth subordinate unit (host name `head_office_cle`, priority 4, weight 30)

Dynamic weighted load balancing

You can configure active-active HA weighted round robin load balancing to load balance sessions according to individual cluster unit CPU usage, memory usage, and number of UTM proxy sessions. If any of these system loading indicators increases above configured high watermark thresholds, weighted load balancing sends fewer new sessions to the busy unit until it recovers.

For example, if you set a CPU usage high watermark, when a cluster unit's CPU usage reaches the high watermark threshold fewer sessions are sent to it. With fewer sessions to process the cluster unit's CPU usage should fall back to a low watermark threshold. When this happens the cluster resumes load balancing sessions to the cluster unit as normal.

You can set different high and low watermark thresholds for CPU usage and memory usage, and for the number of HTTP, FTP, IMAP, POP3, SMTP, or NNTP UTM proxy sessions. For each loading indicator you set a high watermark threshold a low watermark threshold and a weight. When you first enable this feature the weighted load balancing configuration is synchronized to all cluster units. Subsequent changes to the weighted load balancing configuration are not synchronized so you can configure different weights on each cluster unit.

The CPU usage, memory usage, and UTM proxy weights determine how the cluster load balances sessions when a high watermark threshold is reached and also affect how the cluster load balances sessions when multiple cluster units reach different high watermark thresholds at the same time. For example, you might be less concerned about a cluster unit reaching the memory usage high watermark threshold than reaching the CPU usage high watermark threshold. If this is the case you can set the weight lower for memory usage. Then, if one cluster unit reaches the CPU usage high watermark threshold and a second cluster unit reaches the memory usage high watermark threshold the cluster will load balance more sessions to the unit with high memory usage and fewer sessions to the cluster unit with high CPU usage.

Use the following command to set thresholds and weights for CPU and memory usage and UTM proxy sessions:

```
config system ha
  set mode a-a
  set schedule weight-round-robin
  set cpu-threshold <weight> <low> <high>
  set memory-threshold <weight> <low> <high>
  set http-proxy-threshold <weight> <low> <high>
  set ftp-proxy-threshold <weight> <low> <high>
  set imap-proxy-threshold <weight> <low> <high>
  set nntp-proxy-threshold <weight> <low> <high>
  set pop3-proxy-threshold <weight> <low> <high>
  set smtp-proxy-threshold <weight> <low> <high>
end
```

For each option, the weight range is 0 to 255 and the default weight is 5. The low and high watermarks are a percent (0 to 100). The default low and high watermarks are 0 which means they are disabled. The high watermark must be greater than the low watermark.

For CPU and memory usage the low and high watermarks are compared with the percentage CPU and memory use of the cluster unit. For each of the UTM proxies the high and low watermarks are compared to a number that represents percent of the max number of proxy sessions being used by a proxy. This number is calculated using the formula:

```
proxy usage = (current sessions * 100) / max sessions
```

where:

`current sessions` is the number of active sessions for the proxy type.

`max sessions` is the session limit for the proxy type. The session limit depends on the FortiGate unit and its configuration.

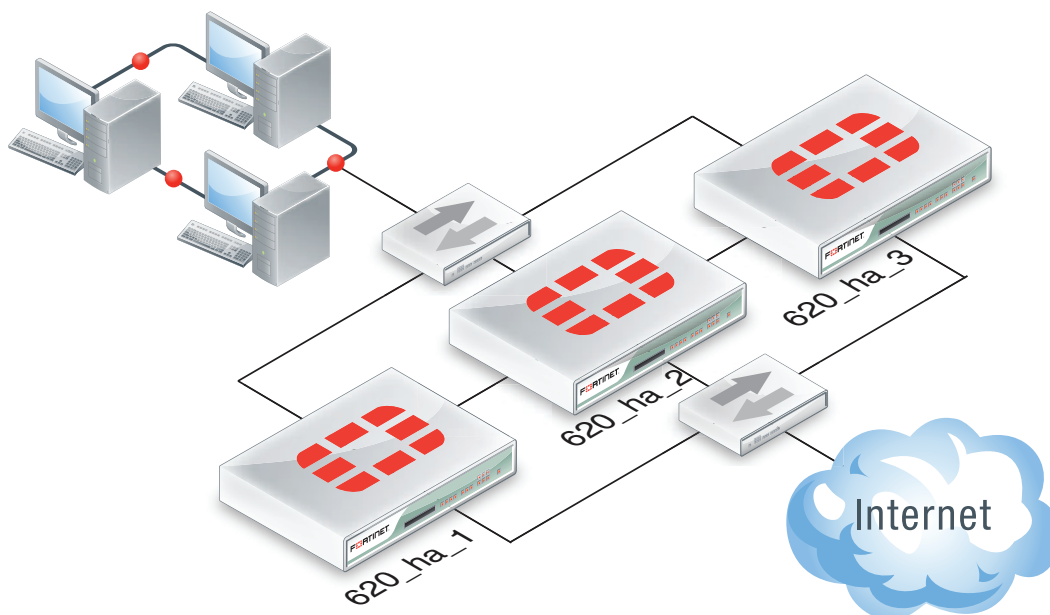
You can use the following command to display the maximum and current number of sessions for a UTM proxy:

```
get test {ftpd | http | imap | nntp | pop3 | smtp} 4
```

Example weighted load balancing configuration

Consider a cluster to three FortiGate-620B units with host names `620_ha_1`, `620_ha_2`, and `620_ha_3` as shown in Figure 15. This example describes how to configure weighted load balancing settings for CPU and memory usage for the cluster and then to configure UTM proxy weights for each cluster unit.

Figure 15: Example HA weighted load balancing configuration



Use the following command to set the CPU usage threshold weight to 30, low watermark to 60, and high watermark to 80. This command also sets the memory usage threshold weight to 10, low watermark to 60, and high watermark to 90.

```
config system ha
  set mode a-a
  set schedule weight-round-robin
  set cpu-threshold 30 60 80
  set memory-threshold 10 60 90
end
```

The static weights for the cluster units remain at the default values of 40. Since this command changes the mode to `a-a` and the schedule to `weight-round-robin` the weight settings are synchronized to all cluster units.



For FortiOS 4.0 MR3, the static weights assigned to cluster units using the `set weight` have changed. The default value is 40 and the range is now 0 to 255.

As a result of this configuration, if the CPU usage of `620_ha_1` reaches 80% the static weight for `620_ha_1` is reduced from 40 to 10 and correspondingly fewer sessions are load balanced to it. If the memory usage of this same cluster unit also reaches 90% the static weight further reduces to 0 and no new sessions are load balanced to it. If the memory usage of a `620_ha_2` reaches 90% the static weight of `620_ha_2` reduces to 30 and 30 and fewer new sessions are load balanced to it.

Now that you have set the basic weighted load balancing configuration for the cluster you can configure different settings on each cluster unit. For example, to set the HTTP usage threshold weight to 20, low watermark to 60, and high watermark to 90 for `620_ha_2` use the `execute ha manage` command to log into the `620_ha_2` CLI. Then enter the following command:

```
config system ha
  set http-proxy-threshold 20 60 90
end
```

To set the pop3 usage threshold weight to 20, low watermark to 60, and high watermark to 90 for `620_ha_3` use the `execute ha manage` command to log into the `620_ha_3` CLI. Then enter the following command:

```
config system ha
  set pop3-proxy-threshold <weight> <low> <high>
end
```

VRRP virtual MAC address support

Previously in FortiOS 4.0 MR2, the VRRP virtual MAC address (also known as the virtual router MAC address) feature, as described in [RFC 3768](#), **was supported**. The VRRP virtual MAC address is a shared MAC address adopted by the VRRP master. If the VRRP router group master fails the same virtual MAC master fails over to the new master of the group. As a result, all packets for VRRP routers can continue to use the same virtual MAC address. You must enable the VRRP virtual MAC address feature on all members of a VRRP group.

Each VRRP router is associated with its own virtual MAC address. The last part of the virtual MAC depends on the VRRP virtual router ID using the following format:

```
00-00-5E-00-01-<VRID_hex>
```

Where `<VRID_hex>` is the VRRP virtual router ID in hexadecimal format in internet standard bit-order. For more information about the format of the virtual MAC see RFC 3768.

Some examples:

- If the VRRP virtual router ID is 10 the virtual MAC would be 00-00-5E-00-01-05.
- If the VRRP virtual router ID is 200 the virtual MAC would be 00-00-5E-00-01-c8.

The VRRP virtual MAC address feature is disabled by default. When you enable the feature on a FortiGate interface, all of the VRRP routers added to that interface use their own VRRP virtual MAC address. Each virtual MAC address will be different because each virtual router has its own ID.

Use the following command to enable the VRRP virtual MAC address on the port2 interface and add a VRRP virtual router with ID 5, IP address 10.31.101.120 and priority 255.

```
config system interface
  edit port2
    set vrrp-virtual-mac enable
  config vrrp
    edit 5
      set vrip 10.31.101.120
      set priority 255
    end
  end
end
```

The port2 interface will now accept packets sent to the MAC address 00-00-5E-00-01-05.

FGCP HA subsecond failover

FGCP HA subsecond failover (that is a failover time of less than one second) can reduce the failover time after a device or link failover. In FortiOS 4.0 MR3 the CLI option for configuring subsecond failover has been removed and the feature is available for interfaces that include:

- Network processors: NP2, NP4
- Content processors: CP4, CP5, CP6
- Accelerated interfaces, for example the ASM-FB4, ADM-FB8, ADM-XB2, ADM-XD4, RTM-XD2
- Security processor modules: ASM-CE4, ASM-XE2

Subsecond failover can accelerate HA failover depending on the FortiGate unit HA and hardware configuration and the network configuration. Network devices that respond slowly to an HA failover can prevent this feature from reducing failover times to less than a second. Also, subsecond failover can normally only be achieved for a cluster of two units operating in Transparent mode with only two interfaces connected to the network.

For best subsecond failover results, the recommended heartbeat interval is 100ms and the recommended lost heartbeat threshold is 5.

```
config system ha
  set hb-lost-threshold 5
  set hb-interval 1
end
```

Static Route enhancements

Static routes now provides *Priority* and *Distance* settings in the Advanced section on the New Static Route page. The priority and distance settings can be displayed on the Static Route page using *Column Settings*. The priority and distance columns do not appear by default.

Figure 16: The Static Route page with the priority and distance columns displayed

+ Create New		Edit	Delete	[Column Settings]		
	IP/Mask	Gateway	Device	Comment	Priority	Distance
<input type="checkbox"/>	0.0.0.0/0.0.0.0	0.0.0.0	wan2		0	10
<input type="checkbox"/>	172.20.120.0/255.255.255.0		ssl.root	for VPN SSL	400	155

When configuring a static route (or when modifying its settings), you can now include a comment within the static route. If you want to configure the priority and/or distance within a static route, you must select *Advanced...* to display priority and distance options.

Monitoring ISIS from the Routing Monitor page


You can now view ISIS routes from the Routing Monitor page. ISIS, introduced in FortiOS 4.0 MR2, is a routing protocol described in RFC 1142. ISIS is configured within the CLI.

Security Policy and Firewall Object Enhancements

There are several enhancements to firewall policies, including the Policy page (in *Policy > Policy > Policy*), which provides more flexibility and granularity. These enhancements also include page controls on the Address page in *Firewall Objects > Address > Address* to easily navigate through the list of addresses on the page.

The Firewall menu also provides more granularity when configuring a schedule. When configuring a schedule, you can now specify minutes in five minute intervals, for example, 5, 10, 15, 20, and all the way up to 55.

In FTP proxy security policies, FSSO guest user groups are now supported. FSSO authentication is IP-based authentication.



Traffic shaping bandwidth is now in kbits.

Source IP addresses for FortiGate-originating traffic

Previously, the source IP address feature was introduced in FortiOS 4.0MR2. In this release the source-ip address is extended, adding more options for configuring a source IP address to self-originating traffic. For example, NTP.

The source-ip address feature allows you to specify the source IP address of self-originating traffic.

This feature is configured only in the CLI. A source IP address can be configured for NTP FortiGuard, DNS, RADIUS, TACACS+, and FSSO.

You can use the `get system source-ip status` command to view the services that force their communication to use a specific source IP address.

Example of using the source IP address feature to track logs at a syslog server

Management wants to be able to track logs at a syslog server. There are five log devices; two FortiAnalyzer units that are being used for archival purposes, and three Syslog servers that store all other log files. All log devices have been configured and you must edit the existing Syslog server configuration for the Syslog server that management wants tracked, `syslog_2`. The source IP address is `172.20.120.155`.

To include the source IP address to track logs in the existing configuration

- 1 Log in to the CLI.
- 2 Enter the following command:


```
config log syslog2 setting
```
- 3 In the `syslog_2` configuration, enter the following commands:


```
set source-ip 172.20.120.155
end
```
- 4 View the services for `syslog_2` using the following command:


```
get system source-ip status
```

Local-in security policies

Local-in security policies are policies that are designed for traffic that is FortiGate-oriented. For example, central management. There are already local-in policies, which are automatically set up by the FortiGate unit. These policies include central-management, update announcement, and Netbios forward.

When configuring security policies for local-in traffic, the destination address is limited to the FortiGate interface IP and secondary IP addresses. Local-in policies are used in a backward compatible way with `allow-access`. These security policies are configured only in the CLI. You can configure local-in security policies for both IPv4 and IPv6.

The following are the commands used to configure a local-in security policy:

```
config firewall policy
edit <integer>
set intf <source_interface_name>
set srcaddr <source_address_name>
set dstaddr <destination_address_name>
set action {accept | deny}
set service <service_name>
set schedule <schedule_type>
set auto-asic-offload {enable | disable}
set status {enable | disable}
end
```

Protocol Options

When accessing *Policy > Policy > Protocol Options*, you will notice that you are directed to the Edit Protocol Options page. This page is referred to as the Configuration Settings page, similar to how the UTM profiles and sensors are accessed. A default protocol options list is available as well as your configured protocol options lists.

You can create a new protocol option list from the Configuration Settings page by selecting the *Create New* icon. If you want to view a list of all protocol option lists, select the *View List* icon. You can access a protocol option list at any time on the Settings page by selecting one from the drop-down list beside the *Create New* icon.

FTPS support

FTPS is now supported within the Protocol Options page as well as within the UTM features. This support extends the SSL proxy so that decrypted FTPS data can be examined by the proxies.

Virtual IP source address filter support

In *Firewall Objects > Virtual IP > Virtual IP*, you can now add multiple source IP addresses for filtering purposes. This feature allows packets from different sources to be translated to different VIPs. By default, the filter is set to 0.0.0.0, which means that all source IP addresses provide a backward compatibility. The mapped IP address range is also set to 0.0.0.0 by default.

When you enter the mapped IP address for the mapped range for source address filter, the FortiGate unit automatically calculates the range.

Virtual IP port forwarding enhancements

The VIP port forwarding feature (*Firewall Objects > Virtual IP > Virtual IP*) has been enhanced so that you can easily enter the external service port range first. The FortiGate unit calculates the mapped port range after you enter the start of the port range.

You must select *Port Forwarding* to reveal the configuration settings for port forwarding as well as enable it.

Load balancing HTTP host connections

Load balancing for HTTP host connections can be used for load balancing across multiple real servers using the host's HTTP header to guide the connection to the correct real server, providing better load balancing for those connections. The HTTP host can be configured either in the CLI or web-based manager, in *Firewall Objects > Load Balance > Virtual Server*.

The load balancing method used is called http-host. When selected in the CLI, this allows a real server to specify a http-host attribute which is the domain name of the traffic for that real server. For example, a FortiGate unit is load balancing traffic to three real servers; traffic for www.example.com should go to 10.10.10.1, traffic for www.example.org should go to 10.10.10.5, and traffic for any other domain should go to 10.10.10.100.

Web Proxy Service and Web Proxy Service Group

There are two new menus in *Firewall Objects > Service*: Web Proxy Service and Web Proxy Group.

The Web Proxy Service menu provides configuration settings for web proxy services that can then be applied to a security policy. Web proxy services are similar to custom services, where you can configure the services to define one or more protocols and port numbers that are associated with each web proxy service. Web proxy services can also be grouped, in *Firewall Objects > Service > Web Proxy Service Group*.

The Web Proxy Service Group menu, similar to the Group menu, provides configuration settings for grouping the configured web proxy services. By grouping web proxy services, you can apply multiple services to a security policy.

SSL renegotiation for SSL offloading provides allow/deny client renegotiation

FortiOS now supports SSL offloading that either allows or denies client renegotiation. This feature helps to resolve the issue that affects all SSL and TLS servers that support renegotiation, which was identified by the Common Vulnerabilities and Exposures system, in [CVE-2009-3555](#). The IETF is working on a TLS protocol change that will permanently fix the issue and until they implement the change, the allow and deny client renegotiation feature in FortiOS provides a workaround. This workaround allows you to disable support for SSL/TLS renegotiation in a server, for the SSL offloading feature.

The configuration is in the CLI:

```
config firewall vip
    set ssl-client-renegotiation {allow | deny}
end
```

The allow option is enabled by default for backwards capability. If you choose deny, as soon as a “ClientHello” message (indicating a renegotiation) is received from the client, the server terminates the TCP connection.

You can test the renegotiation behavior using OpenSSL. The OpenSSL client application has a request feature that it can do renegotiation, by typing “R”. When you use this feature, the `diag debug appl vs -1` can be used to view the renegotiation where deny is used.

SSL VPN Port forwarding support

You can now configure port forwarding for Citrix, native RDP and general port forwarding for portals for web mode. The configuration settings are found in the Portal Settings page, in the Settings Window. These port forwarding settings are also available in the CLI.

IKE negotiation

The IKE negotiation process now provides options for how the negotiation is controlled when there is no traffic, as well as how long the FortiGate unit waits for the negotiation to occur. Within the CLI, two new commands help you to configure the `negotiation-timeout` (which is new) and `auto-negotiation` which now replaces `auto-keepalive` or `set keepalive {enable | disable}`.

The `auto-negotiation` command controls whether IKE is negotiation even when there is no traffic. This command would usually be used where there is multiple redundant or overlapping tunnels and there is a need to have the primary connection established. When enabled, the FortiGate unit keeps trying to negotiation IKE event if the link is down and traffic is flowing over a secondary tunnel.

For `auto-negotiation`, if the previous configuration has DPD enabled, the upgrade process automatically enables auto-negotiation so that the behavior is the same as previously configuration.

The `negotiation-timeout` command controls how long the FortiGate unit waits for IKE to negotiate, similar to the web-based manager’s timeout settings. The default time is 30 seconds. If DPD was enabled in a previous configuration, the `negotiate-timeout` settings will be that of the `dpd-retrycount` and `dpd-retryinterval` so that the FortiGate unit will time out connections at the same rate as they would have in the previous build.

SHA-384 and SHA-512 support for IKE

For IPsec, you can now choose either SHA-384 or SHA-512 when configuring IPsec. These authentication algorithms are available for IKE (including phase 1 and phase 2), and manual key configurations.

In the web-based manager, both *Authentication Algorithm* and *Encryption Algorithm* drop-down lists provide the SHA-384 and SHA-512 options for IPsec.

FortiOS Carrier URL extraction feature

The URL extraction feature extracts the embedded Uniform Resource Identifier (URI) within the path for only the host that is specified. The feature applies to HTTP requests for URLs. For example, the URI “http://example.proxy.com/http://www.example.com”; when the URI is broken down, you find the FQDN (example.proxy.com) and the path (http://www.example.com).

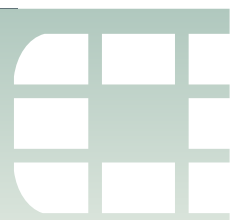
The URL extraction feature, however, does not extract the URL if its a regular HTTP request, such as http://example.proxy.com/examples/example.html. The feature also does not extract a URL if the request does not match the FQDN of the proxy server.

This feature is available within a web filter profile, under *URL Extraction*. You must select the *Enable URL Extraction* check box to enable it and access the other settings. The settings that you can choose from are:

- *URL Extraction proxy server FQDN* – the proxy server hostname, such as FQDN, for which the URL extraction will apply. The proxy server hostname must be entered in the field.
- *Blocked page redirect header name* – HTTP header name that is used for client redirect on blocked requests.
- *Blocked page redirect header value (URL)* – HTTP header value that is used for client redirect on blocked requests.

You can also use the CLI command `redirect-no-content` which behaves in the following way:

- `enabled` – if extracted URL is blocked by this feature, the HTTP response contains no content, for example message body is no present.
- `disabled` – the value from Blocked Page redirect header name configuration includes both the redirect header and the message body.



Appendix

Document conventions

Fortinet technical documentation uses the conventions described below.

IPv4 IP addresses

To avoid publication of public IPv4 IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at <http://ietf.org/rfc/rfc1918.txt?number-1918>.

Most of the examples in this document use the following IP addressing:

IP addresses are made up of A.B.C.D:

- A - can be one of 192, 172, or 10 - the private addresses covered in RFC 1918.
- B - 168, or the branch / device / virtual device number.
 - Branch number can be 0xx, 1xx, 2xx - 0 is Head office, 1 is remote, 2 is other.
 - Device or virtual device - allows multiple FortiGate units in this address space (VDOMs).
 - Devices can be from x01 to x99.
- C - interface - FortiGate units can have up to 40 interfaces, potentially more than one on the same subnet
 - 001 - 099- physical address ports, and non -virtual interfaces
 - 100-255 - VLANs, tunnels, aggregate links, redundant links, vdom-links, etc.
- D - usage based addresses, this part is determined by what the device is doing. The following gives 16 reserved, 140 users, and 100 servers in the subnet.
 - 001 - 009 - reserved for networking hardware, like routers, gateways, etc.
 - 010 - 099 - DHCP range - users
 - 100 - 109 - FortiGate devices - typically only use 100
 - 110 - 199 - servers in general (see later for details)
 - 200 - 249 - static range - users
 - 250 - 255 - reserved (255 is broadcast, 000 not used)
 - The D segment servers can be farther broken down into:
 - 110 - 119 - Email servers
 - 120 - 129 - Web servers
 - 130 - 139 - Syslog servers
 - 140 - 149 - Authentication (RADIUS, LDAP, TACACS+, FSAE, etc)
 - 150 - 159 - VoIP / SIP servers / managers
 - 160 - 169 - FortiAnalyzers
 - 170 - 179 - FortiManagers
 - 180 - 189 - Other Fortinet products (FortiScan, FortiDB, etc.)
 - 190 - 199 - Other non-Fortinet servers (NAS, SQL, DNS, DDNS, etc.)
 - Fortinet products, non-FortiGate, are found from 160 - 189.

Example Network

Variations on network shown in [Figure 17](#) are used for many of the examples in this document. In this example, the 172.20.120.0 network is equivalent to the Internet. The network consists of a head office and two branch offices.

Figure 17: Example network

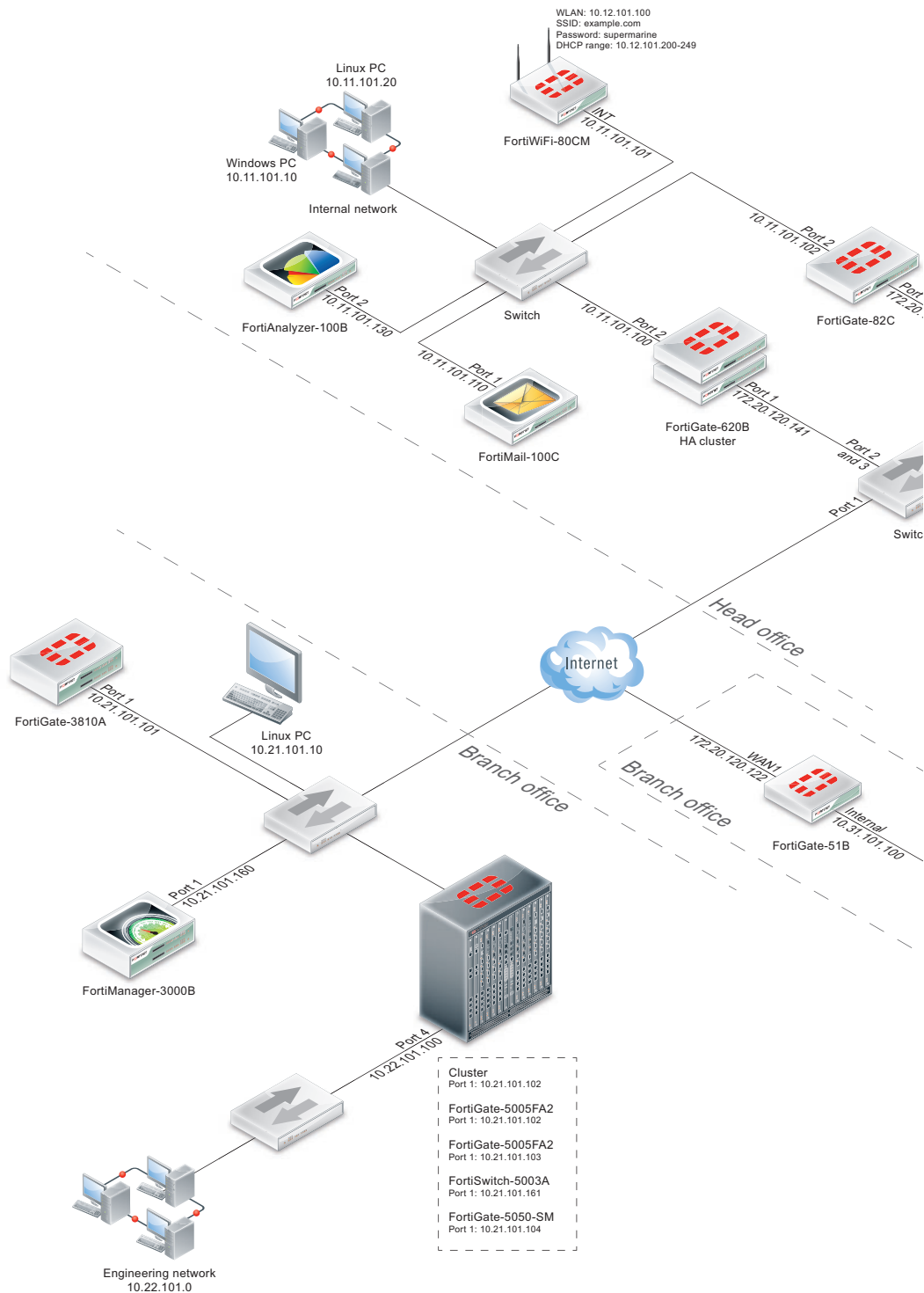




Table 4: Example IPv4 IP addresses

Location and device	Internal	Dmz	External
Head Office, one FortiGate	10.11.101.100	10.11.201.100	172.20.120.191
Head Office, second FortiGate	10.12.101.100	10.12.201.100	172.20.120.192
Branch Office, one FortiGate	10.21.101.100	10.21.201.100	172.20.120.193
Office 7, one FortiGate with 9 VDOMs	10.79.101.100	10.79.101.100	172.20.120.194
Office 3, one FortiGate, web server	n/a	10.31.201.110	n/a
Bob in accounting on the corporate user network (DHCP) at Head Office, one FortiGate	10.0.11.101.200	n/a	n/a
Router outside the FortiGate	n/a	n/a	172.20.120.195


Tips, must reads, and troubleshooting



A Tip provides shortcuts, alternative approaches, or background information about the task at hand. Ignoring a tip should have no negative consequences, but you might miss out on a trick that makes your life easier.



A Must Read item details things that should not be missed such as reminders to back up your configuration, configuration items that must be set, or information about safe handling of hardware. Ignoring a must read item may cause physical injury, component damage, data loss, irritation or frustration.



A Troubleshooting tip provides information to help you track down why your configuration is not working.

Typographical conventions

Table 5: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<code>config system dns set primary <address_ipv4> end</code>
CLI output	<code>FGT-602803030703 # get system settings comments : (null) opmode : nat</code>

Table 5: Typographical conventions in Fortinet technical documentation

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

Registering your Fortinet product

Access to Fortinet customer services, such as firmware updates, support, and FortiGuard services, requires product registration. You can register your Fortinet product at <http://support.fortinet.com>.

Training Services

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

Visit Fortinet Training Services at <http://campus.training.fortinet.com>, or email training@fortinet.com.

Technical Documentation

Visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>, for the most up-to-date technical documentation.

The Fortinet Knowledge Base provides troubleshooting, how-to articles, examples, FAQs, technical notes, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

Comments on Fortinet technical documentation

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

Customer service and support

Fortinet is committed to your complete satisfaction. Through our regional Technical Assistance Centers and partners worldwide, Fortinet provides remedial support during the operation phase of your Fortinet product's development life cycle. Our Certified Support Partners provide first level technical assistance to Fortinet customers, while the regional TACs solve complex technical issues that our partners are unable to resolve.

Visit Customer Service and Support at <http://support.fortinet.com>.

Fortinet products End User License Agreement

See the [Fortinet products End User License Agreement](#).



Index

Numerics

3G/4G modem list, 24

A

access profiles
 VDOM and global privileges, 88
 access profiles, example
 VDOM and global privileges, 88
 adding tags to firewall policies and address lists, 69
 adding tags to predefined signatures and application, 70
 antivirus profiles, archive inspection, 17
 Application Monitor submenu, 64
 application sensor, 19
 Archive & Data Leak Monitor submenu, 63
 archive inspection for antivirus profiles, 17
 asset definition, 34
 authorize-manager-only, CLI, 78
 automatic radio resource provisioning ARRP, 26
 AV Monitor submenu, 63

B

backing up and restoring, per VDOM, 71
 backing up config file, 12

C

certification, 104
 chart display, 61
 chat message log, MSNP21, 54
 CLI
 authorize-manager-only, 78
 custom maximum invalid firewall auth attempts, 81
 customize number of invalid firewall auth attempts, 81
 DDNS commands, 78
 deleting all local logs, archives and user-configured report templates, 56
 example for uploading logs to FTP server (text format), 55
 get commands, traffic shaper and per-IP shaper, 80
 management checksum config for FortiManager, 80
 MTU config support (non-IPsec tunnels), 81
 netscan asset auth, 34
 NTLM authentication, 33
 OSPFv3 NSSA extension, 35
 real-time session, traffic shaper bandwidth and CP6 statistics, 78
 SSL connection encrypt level option, 54
 uploading logs to FTP server (text format), 55
 WiFi, user group authentication, 27
 config file, backing up, 12
 controlling connection between FortiGate and FortiManager, CLI, 81

conventions, 101
 CP6 statistics, diag, CLI, 78
 CPU usage
 weight, 91
 cpu usage
 weighted load balancing, 91
 custom maximum invalid firewall auth attempts, CLI, 81
 customer service, 104
 customize number of invalid firewall auth attempts, CLI, 81

D

DHCP ipv6, 36
 DHCP Monitor submenu, 61
 DHCP server, 84
 IP Reservation, 84
 ipv6, 36
 diag system icap profile list , ICAP, 23
 diag system icap server list , ICAP, 23
 distributed ARRP, 26
 DLP archives, sending to multiple FortiAnalyzer units, 52
 DLP document fingerprinting, 20
 DNS server, 83
 documentation
 conventions, 101
 Fortinet, 104
 downloading log messages in Log Access, 50
 dynamic DNS, CLI, 78
 dynamic profile, 31

E

Email Monitor submenu, 63
 endpoint control, 33
 endpoint security
 endpoint control, 33
 event logs, 53
 event-system logs, 54
 example for two-factor authentication, 29
 example for VDOM and global privileges for access profiles, 88
 example of source IP address, FortiGate-originating traffic, 95
 explicit FTP proxy
 replacement message, 37
 explicit proxy
 authentication cookie for session-based authentication, 38
 form-based user authentication, 38
 forwarding servers, 37
 FTP, 36
 explicit web proxy
 proxy chaining, 37

F

- failover
 - subsecond, 94
- FAMS, 41
- filtering lists, 65
- filtering log messages, 50
- firewall
 - protocol options, 96
 - virtual IP port forwarding, 97
 - virtual IP source address filter, 97
- firewall address
 - geography-based filtering, 19
- firewall address lists
 - adding tags, 69
- firewall configuration object icons, 71
- firewall objects, 57
- firewall policies
 - adding tags, 69
 - local-in, 96
- firewall policy
 - See security policy, 57
- firmware practices, 11
- flow-based DLP, 16
- flow-based web filtering, 15
- formatting multiple disk partitions, 82
- form-based user authentication, explicit proxy, 38
- FortiClient Connect, 77
- FortiExplorer, 58
- FortiGate
 - dynamic profile, 31
 - source IP address, 95
- FortiGate setup wizard, 58
- FortiGuard
 - Antivirus, 104
- FortiGuard, 3G/4G modem list, 24
- Fortinet
 - Technical Documentation, conventions, 101
 - Technical Support, 104
 - Technical Support, registering with, 104
 - Training Services, 104
- Fortinet customer service, 104
- Fortinet documentation, 104
- FortiOS Carrier
 - URL extraction, 99
- FortiToken, 28
- forwarding servers, 37
- FTP proxy
 - change the prompt, 37
- FTPS, 96

G

- geography-based filtering, firewall address, 19

H

- HA
 - configure weighted-round-robin weights, 89
- HA dynamic weighted load balancing
 - dynamic weighted load balancing, 91
 - weighted-round-robin weights, 89

I

- ICAP, 21
 - example of ICAP, 23
 - troubleshooting, 23
- IKE negotiation, 98
- installing firmware on a partition without a reboot, 84
- introduction
 - Fortinet documentation, 104
- Intrusion Monitor submenu, 63
- IP address
 - private network, 101
- IP Reservation, 84
- IPS
 - predefined signature viewer table, 17
- IPS signature threshold, 17
- IPsec
 - IKE negotiation, 98
- IPsec Monitor submenu, 64

L

- load balance
 - cpu usage, 91
 - memory usage, 91
 - proxy UTM sessions, 91
- Load Balance Monitor submenu, 62
- load balancing
 - HTTP host connections, 97
- load balancing HTTP host connections, 97
- local-in firewall policies, 96
- Logging Monitor submenu, 53
- login grace timer for SSH connections, 78
- logs
 - chat message support for MSNP21, 54
 - other-traffic, 54

M

- MAC address
 - VRRP virtual, 93
- management checksum, FortiManager, 80
- memory usage
 - weight, 91
 - weighted load balancing, 91
- MIB
 - wan opt, web cache and explicit proxy, 86
- Modem Monitor submenu, 62
- monitor
 - WAN Optimization peers, 64
 - web cache, 64

Monitor submenus

- Application Monitor, 64
- Archive & Data Leak Monitor, 63
- AV Monitor, 63
- DHCP Monitor, 61
- Email Monitor, 63
- Intrusion Monitor, 63
- IPsec Monitor, 64
- Load Balance Monitor, 62
- Logging Monitor, 53
- Modem Monitor, 62
- Policy Monitor, 62
- Session Monitor, 62
- SSL-VPN Monitor, 64
- Traffic Shaper Monitor, 62
- Web Monitor, 63

monitor submenus, 61

monitoring ISIS, 95

MTU config support (non-IPsec tunnels), CLI, 81

multiple group enforcement, 31

N

netscan asset auth, CLI, 34

network protocol usage, 60

network vulnerability scan

- asset definition, 34

- scan schedule, 34

- vulnerability result, 34

NTLM authentication, CLI, 33

O

OSPFv3 NSSA extension, CLI, 35

other-traffic logs, 54

overrides

- web filtering, 18

P

peer

- WAN Optimization monitor, 64

per-IP shaper, CLI, 80

PKI certificate authentication, 32

policy

- menu, 57

Policy Monitor submenu, 62

port pair (transparent mode), 83

practices, firmware upgrade, 11

predefined signature viewer table, 17

predefined signatures

- adding tags, 70

product registration, 104

profile group, 23

protocol options, 96

- FTPS support, 96

proxy chaining

- explicit web proxy, 37

proxy forwarding server

- explicit web proxy, 37

proxy UTM sessions

- weighted load balancing, 91

R

real-time session, diag, CLI, 78

reference count column, 66

registering

- with Fortinet Technical Support, 104

remote logging configuration settings, 52

replacement message

- explicit FTP proxy, 37

replacement messages

- archive and FTP proxy, 87

- images, 87

- successful firewall authentication, 87

- video chat block, 87

- web filtering disclaimer, 87

RFC

- 1918, 101

S

scan schedule, 34

security policy

- firewall policy, 57

- web cache support, 38

Session Monitor submenu, 62

setup wizard, 58

SNMP

- v3, 86

source IP address, FortiGate-originating traffic, 95

SSH connections

- login grace timer, 78

SSL connection encrypt level option, CLI, 54

SSL renegotiation for SSL offloading, 98

SSL, port forwarding, 98

SSL-VPN Monitor submenu, 64

static route enhancement, 94

static weight, 89

sub second failover, 94

sub-second failover, 94

subsecond failover, 94

suppressing rogue AP, 26

system resources, 59

T

tag management, 68

technical

- documentation conventions, 101

- support, 104

technical support, 104

test upgrade procedure, 12

timeout enhancement, authentication, 32

top session ipv6 support, 35

traffic history, 59

traffic shaper bandwidth, diag, CLI, 78

Traffic Shaper Monitor submenu, 62

traffic shaper, CLI, 80

Training Services, 104

transparent mode, port pair, 83

two-factor authentication, 29

two-factor authentication for administrators, 30

two-factor authentication, example, 29

U

upgrade practices, 11
uploading logs to FTP server (text format), CLI, 55
URL extraction, FortiOS Carrier, 99
using test procedure to install firmware, 12
UTM profiles, 57
UTM proxy
 weight, 91

V

VDOM
 backing up and restoring, 71
VDOM and global privileges for access profiles, 88
video chat block replacement message, 87
viewing log messages in Log Access, 49
viewing reports, 48
virtual MAC address
 VRRP, 93
virtual router MAC address
 VRRP, 93
VRRP
 virtual MAC address, 93
vulnerability result, 34

W

web cache
 monitor, 64
web cache, security policy, 38
web filtering overrides, 18
Web Monitor submenus, 63
web proxy service, 97
web proxy service group, 97
web-based manager
 tag management, 68
web-based manager, filtering lists, 65
weight
 static, 89
weighted-round-robin
 configuring weights, 89
widgets
 network protocol usage, 60
 system resources, 59
 top session, 35
 traffic history, 59
WiFi, CLI, 27
wireless controller
 suppressing rogue AP, 26
wizard, setup, 58