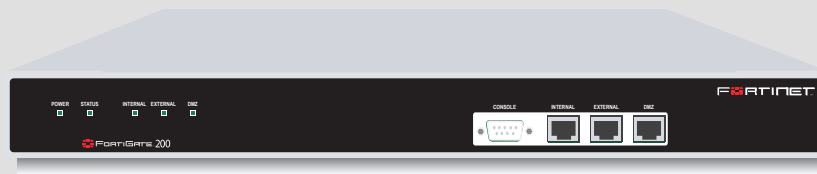


**FORTINET**™

**FortiGate 200**

**Administration Guide**



## **FortiGate-200 Administration Guide**

**Version 2.80 MR7**

**3 December 2004**

**01-28007-0004-20041203**

© Copyright 2004 Fortinet Inc. All rights reserved.

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

*FortiGate-200 Administration Guide*

Version 2.80 MR7

3 December 2004

01-28007-0004-20041203

### **Trademarks**

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

### **Regulatory Compliance**

FCC Class A Part 15 CSA/CUS

CAUTION: RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.  
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.

For technical support, please visit <http://www.fortinet.com>.

Send information about errors or omissions in this document or any Fortinet technical documentation to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

# Table of Contents

<b>Introduction .....</b>	<b>13</b>
About FortiGate Antivirus Firewalls.....	13
Antivirus protection .....	14
Web content filtering .....	14
Spam filtering .....	15
Firewall.....	15
VLANs and virtual domains.....	16
Intrusion Prevention System (IPS).....	17
VPN.....	17
High availability .....	18
Secure installation, configuration, and management .....	18
Document conventions .....	19
FortiGate documentation .....	21
Fortinet Knowledge Center .....	21
Comments on Fortinet technical documentation.....	21
Related documentation .....	22
FortiManager documentation .....	22
FortiClient documentation .....	22
FortiMail documentation.....	22
FortiLog documentation .....	23
Customer service and technical support.....	23
 <b>System status.....</b>	 <b>25</b>
Console access.....	25
Status.....	26
Viewing system status .....	26
Changing unit information .....	29
Session list.....	32
Changing the FortiGate firmware.....	33
Upgrading to a new firmware version .....	33
Reverting to a previous firmware version.....	35
Installing firmware images from a system reboot using the CLI .....	38
Testing a new firmware image before installing it .....	41
Installing and using a backup firmware image .....	43
 <b>System network .....</b>	 <b>47</b>
Interface .....	47
Interface settings.....	48
Configuring interfaces .....	53
Zone.....	58
Zone settings .....	58

Management .....	59
DNS .....	61
Routing table (Transparent Mode) .....	61
Routing table list .....	61
Transparent mode route settings .....	62
VLAN overview .....	62
FortiGate units and VLANs .....	63
VLANs in NAT/Route mode .....	63
Rules for VLAN IDs .....	64
Rules for VLAN IP addresses .....	64
Adding VLAN subinterfaces .....	65
VLANs in Transparent mode .....	66
Rules for VLAN IDs .....	68
Transparent mode virtual domains and VLANs .....	68
Transparent mode VLAN list .....	69
Transparent mode VLAN settings .....	69
FortiGate IPv6 support .....	71
<b>System DHCP .....</b>	<b>73</b>
Service .....	73
DHCP service settings .....	74
Server .....	75
DHCP server settings .....	76
Exclude range .....	77
DHCP exclude range settings .....	78
IP/MAC binding .....	78
DHCP IP/MAC binding settings .....	79
Dynamic IP .....	79
<b>System config .....</b>	<b>81</b>
System time .....	81
Options .....	82
HA .....	84
HA configuration .....	85
Configuring an HA cluster .....	90
Managing an HA cluster .....	94
SNMP .....	97
Configuring SNMP .....	97
SNMP community .....	98
FortiGate MIBs .....	101
FortiGate traps .....	101
Fortinet MIB fields .....	103

Replacement messages .....	105
Replacement messages list .....	106
Changing replacement messages .....	107
FortiManager.....	108
<b>System administration .....</b>	<b>109</b>
Administrators .....	109
Administrators list.....	110
Administrators options .....	110
Access profiles.....	111
Access profile list .....	112
Access profile options .....	112
<b>System maintenance .....</b>	<b>115</b>
Backup and restore.....	115
Backing up and Restoring.....	116
Update center .....	118
Updating antivirus and attack definitions .....	120
Enabling push updates .....	123
Support .....	125
Sending a bug report .....	126
Registering a FortiGate unit.....	127
Shutdown .....	129
<b>System virtual domain.....</b>	<b>131</b>
Virtual domain properties .....	132
Exclusive virtual domain properties .....	132
Shared configuration settings .....	133
Administration and management .....	134
Virtual domains .....	134
Adding a virtual domain .....	135
Selecting a virtual domain.....	135
Selecting a management virtual domain.....	135
Configuring virtual domains .....	136
Adding interfaces, VLAN subinterfaces, and zones to a virtual domain .....	136
Configuring routing for a virtual domain .....	138
Configuring firewall policies for a virtual domain.....	138
Configuring IPSec VPN for a virtual domain .....	140
<b>Router .....</b>	<b>141</b>
Static.....	141
Static route list .....	143
Static route options .....	144

Policy .....	145
Policy route list.....	145
Policy route options.....	146
RIP .....	146
General .....	147
Networks list.....	148
Networks options .....	149
Interface list.....	149
Interface options .....	150
Distribute list .....	151
Distribute list options.....	152
Offset list .....	153
Offset list options .....	153
Router objects.....	154
Access list .....	154
New access list .....	154
New access list entry .....	155
Prefix list .....	155
New Prefix list .....	156
New prefix list entry.....	157
Route-map list.....	157
New Route-map .....	158
Route-map list entry.....	159
Key chain list.....	160
New key chain.....	160
Key chain list entry.....	161
Monitor.....	162
Routing monitor list .....	162
CLI configuration.....	163
get router info ospf .....	163
get router info protocols .....	163
get router info rip .....	164
config router ospf .....	164
config router static6.....	187

**Firewall..... 189**

Policy .....	190
How policy matching works.....	190
Policy list .....	190
Policy options.....	191
Advanced policy options .....	194
Configuring firewall policies .....	196
Policy CLI configuration .....	197

Address .....	198
Address list .....	199
Address options .....	199
Configuring addresses .....	200
Address group list .....	201
Address group options .....	201
Configuring address groups .....	202
Service .....	203
Predefined service list .....	203
Custom service list .....	206
Custom service options .....	207
Configuring custom services .....	208
Service group list .....	209
Service group options .....	209
Configuring service groups .....	210
Schedule .....	211
One-time schedule list .....	211
One-time schedule options .....	212
Configuring one-time schedules .....	212
Recurring schedule list .....	213
Recurring schedule options .....	213
Configuring recurring schedules .....	214
Virtual IP .....	214
Virtual IP list .....	215
Virtual IP options .....	215
Configuring virtual IPs .....	216
IP pool .....	219
IP pool list .....	220
IP pool options .....	220
Configuring IP pools .....	220
IP Pools for firewall policies that use fixed ports .....	221
IP pools and dynamic NAT .....	221
Protection profile .....	222
Protection profile list .....	222
Default protection profiles .....	223
Protection profile options .....	223
Configuring protection profiles .....	228
Profile CLI configuration .....	229
<b>Users and authentication .....</b>	<b>233</b>
Setting authentication timeout .....	234
Local .....	234
Local user list .....	234
Local user options .....	234

RADIUS .....	235
RADIUS server list .....	235
RADIUS server options .....	236
LDAP .....	236
LDAP server list .....	237
LDAP server options .....	237
User group .....	239
User group list .....	239
User group options .....	240
CLI configuration .....	241
peer .....	241
peergrp .....	242

**VPN..... 245**

Phase 1 .....	246
Phase 1 list .....	246
Phase 1 basic settings .....	247
Phase 1 advanced settings .....	249
Phase 2 .....	250
Phase 2 list .....	251
Phase 2 basic settings .....	251
Phase 2 advanced options .....	252
Manual key .....	253
Manual key list .....	254
Manual key options .....	255
Concentrator .....	256
Concentrator list .....	256
Concentrator options .....	257
Ping Generator .....	257
Ping generator options .....	258
Monitor .....	258
Dialup monitor .....	259
Static IP and dynamic DNS monitor .....	259
PPTP .....	260
PPTP range .....	260
L2TP .....	261
L2TP range .....	261
Certificates .....	262
Local certificate list .....	262
Certificate request .....	263
Importing signed certificates .....	264
CA certificate list .....	265
Importing CA certificates .....	265



VPN configuration procedures .....	266
IPSec configuration procedures .....	266
PPTP configuration procedures .....	268
L2TP configuration procedures .....	268
CLI configuration .....	269
ipsec phase1 .....	269
ipsec phase2 .....	271
ipsec vip .....	272
<b>IPS .....</b>	<b>277</b>
Signature .....	278
Predefined .....	278
Custom .....	282
Anomaly .....	284
Anomaly CLI configuration .....	287
Configuring IPS logging and alert email .....	288
Default fail open setting .....	288
<b>Antivirus .....</b>	<b>289</b>
File block .....	290
File block list .....	291
Configuring the file block list .....	292
Quarantine .....	292
Quarantined files list .....	292
Quarantined files list options .....	293
AutoSubmit list .....	294
AutoSubmit list options .....	294
Configuring the AutoSubmit list .....	294
Config .....	295
Config .....	296
Virus list .....	296
Config .....	296
Grayware .....	297
Grayware options .....	297
CLI configuration .....	299
config antivirus heuristic .....	299
config antivirus quarantine .....	300
config antivirus service http .....	300
config antivirus service ftp .....	302
config antivirus service pop3 .....	304
config antivirus service imap .....	305
config antivirus service smtp .....	307

**Web filter..... 309**

- Content block ..... 311
  - Web content block list ..... 311
  - Web content block options ..... 311
  - Configuring the web content block list ..... 312
- URL block ..... 312
  - Web URL block list..... 313
  - Web URL block options ..... 313
  - Configuring the web URL block list ..... 314
  - Web pattern block list..... 314
  - Web pattern block options ..... 315
  - Configuring web pattern block ..... 315
- URL exempt ..... 315
  - URL exempt list..... 316
  - URL exempt list options ..... 316
  - Configuring URL exempt..... 316
- Category block ..... 317
  - FortiGuard managed web filtering service ..... 317
  - Category block configuration options ..... 318
  - Configuring web category block ..... 319
  - Category block reports ..... 319
  - Category block reports options ..... 320
  - Generating a category block report..... 320
  - Category block CLI configuration ..... 320
- Script filter ..... 321
  - Web script filter options..... 322

**Spam filter ..... 323**

- FortiShield ..... 325
  - FortiShield options ..... 326
  - Configuring the FortiShield cache ..... 326
- IP address ..... 327
  - IP address list ..... 327
  - IP address options ..... 327
  - Configuring the IP address list ..... 328
- RBL & ORDBL ..... 328
  - RBL & ORDBL list..... 329
  - RBL & ORDBL options..... 329
  - Configuring the RBL & ORDBL list ..... 329
- Email address ..... 330
  - Email address list..... 330
  - Email address options..... 330
  - Configuring the email address list..... 331

---

MIME headers.....	331
MIME headers list .....	332
MIME headers options .....	332
Configuring the MIME headers list.....	333
Banned word.....	333
Banned word list .....	334
Banned word options .....	334
Configuring the banned word list .....	335
Using Perl regular expressions.....	335
<b>Log &amp; Report .....</b>	<b>339</b>
Log config .....	340
Log Setting options .....	340
Alert E-mail options.....	344
Log filter options.....	345
Configuring log filters .....	348
Enabling traffic logging.....	348
Log access.....	349
Disk log file access .....	349
Viewing log messages .....	351
Searching log messages.....	353
CLI configuration.....	354
fortilog setting.....	354
syslogd setting .....	355
<b>FortiGuard categories .....</b>	<b>359</b>
<b>Glossary .....</b>	<b>365</b>
<b>Index .....</b>	<b>369</b>



# Introduction

FortiGate Antivirus Firewalls support network-based deployment of application-level services, including antivirus protection and full-scan content filtering. FortiGate Antivirus Firewalls improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network. FortiGate Antivirus Firewalls are ICSA-certified for firewall, IPSec, and antivirus services.

This chapter introduces you to FortiGate Antivirus Firewalls and the following topics:

- [About FortiGate Antivirus Firewalls](#)
- [Document conventions](#)
- [FortiGate documentation](#)
- [Related documentation](#)
- [Customer service and technical support](#)

## About FortiGate Antivirus Firewalls

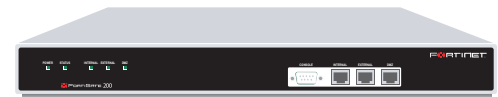
The FortiGate Antivirus Firewall is a dedicated easily managed security device that delivers a full suite of capabilities that include:

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

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

The FortiGate-200 model is an easy-to-deploy and easy-to-administer solution that delivers exceptional value and performance for small office, home office, and branch office applications. The

FortiGate installation wizard guides users through a simple process that enables most installations to be up and running in minutes.



The FortiGate-200 also supports advanced features such as 802.1Q VLANs, virtual domains, high availability (HA), and the RIP and OSPF routing protocols.

## Antivirus protection

FortiGate ICSA-certified antivirus protection scans web (HTTP), file transfer (FTP), and email (SMTP, POP3, and IMAP) content as it passes through the FortiGate unit. FortiGate antivirus protection uses pattern matching and heuristics to find viruses. If a virus is found, antivirus protection removes the file containing the virus from the content stream and forwards a replacement message to the intended recipient.

For extra protection, you can configure antivirus protection to block specified file types from passing through the FortiGate unit. You can use the feature to stop files that might contain new viruses.

FortiGate antivirus protection can also identify and remove known grayware programs. Grayware programs are usually unsolicited commercial software programs that get installed on PCs, often without the user's consent or knowledge. Grayware programs are generally considered an annoyance, but these programs can cause system performance problems or be used for malicious means.

If the FortiGate unit contains a hard disk, infected or blocked files and grayware files can be quarantined. The FortiGate administrator can download quarantined files so that they can be virus scanned, cleaned, and forwarded to the intended recipient. You can also configure the FortiGate unit to automatically delete quarantined files after a specified time.

The FortiGate unit can send email alerts to system administrators when it detects and removes a virus from a content stream. The web and email content can be in normal network traffic or encrypted IPsec VPN traffic.

ICSA Labs has certified that FortiGate Antivirus Firewalls:

- detect 100% of the viruses listed in the current In The Wild List ([www.wildlist.org](http://www.wildlist.org)),
- detect viruses in compressed files using the PKZip format,
- detect viruses in email that has been encoded using uuencode format,
- detect viruses in email that has been encoded using MIME encoding,
- log all actions taken while scanning.

## Web content filtering

FortiGate web content filtering can scan all HTTP content protocol streams for URLs, URL patterns, and web page content. If there is a match between a URL on the URL block list, or a web page contains a word or phrase that is in the content block list, the FortiGate unit blocks the web page. The blocked web page is replaced with a message that you can edit using the FortiGate web-based manager.

FortiGate web content filtering also supports FortiGuard web category blocking. Using web category blocking you can restrict or allow access to web pages based on content ratings of web pages.

You can configure URL blocking to block all or some of the pages on a web site. Using this feature, you can deny access to parts of a web site without denying access to it completely.

To prevent unintentionally blocking legitimate web pages, you can add URLs to an exempt list that overrides the URL blocking and content blocking lists. The exempt list also exempts web traffic this address from virus scanning.

Web content filtering also includes a script filter feature that can block unsecure web content such as Java applets, cookies, and ActiveX.

## Spam filtering

FortiGate spam filtering can scan all POP3, SMTP, and IMAP email content for spam. You can configure spam filtering to filter mail according to IP address, email address, mime headers, and content. Mail messages can be identified as spam or clear.

You can also add the names of known Real-time Blackhole List (RBL) and Open Relay Database List (ORDBL) servers. These services contain lists of known spam sources.

If an email message is found to be spam, the FortiGate adds an email tag to the subject line of the email. The recipient can use the mail client software to filter messages based on the email tag. Spam filtering can also be configured to delete SMTP email messages identified as spam.

## Firewall

The FortiGate ICSA-certified firewall protects your computer networks from Internet threats. ICSA has granted FortiGate firewalls version 4.0 firewall certification, providing assurance that FortiGate firewalls successfully screen and secure corporate networks against a range of threats from public or other untrusted networks.

After basic installation of the FortiGate unit, the firewall allows users on the protected network to access the Internet while blocking Internet access to internal networks. You can configure the firewall to put controls on access to the Internet from the protected networks and to allow controlled access to internal networks.

FortiGate policies include a range of options that:

- control all incoming and outgoing network traffic,
- control encrypted VPN traffic,
- apply antivirus protection and web content filtering,
- block or allow access for all policy options,
- control when individual policies are in effect,
- accept or deny traffic to and from individual addresses,
- control standard and user defined network services individually or in groups,
- require users to authenticate before gaining access,
- include traffic shaping to set access priorities and guarantee or limit bandwidth for each policy,
- include logging to track connections for individual policies,
- include Network Address Translation (NAT) mode and Route mode policies,
- include mixed NAT and Route mode policies.

The FortiGate firewall can operate in NAT/Route mode or Transparent mode.

## NAT/Route mode

In NAT/Route mode, the FortiGate unit is a Layer 3 device. This means that each of its interfaces is associated with a different IP subnet and that it appears to other devices as a router. This is how a firewall is normally deployed.

In NAT/Route mode, you can create NAT mode policies and Route mode policies.

- NAT mode policies use network address translation to hide the addresses in a more secure network from users in a less secure network.
- Route mode policies accept or deny connections between networks without performing address translation.

## Transparent mode

In Transparent mode, the FortiGate unit does not change the Layer 3 topology. This means that all of its interfaces are on the same IP subnet and that it appears to other devices as a bridge. Typically, the FortiGate unit is deployed in Transparent mode to provide antivirus and content filtering behind an existing firewall solution.

Transparent mode provides the same basic firewall protection as NAT mode. The FortiGate unit passes or blocks the packets it receives according to firewall policies. The FortiGate unit can be inserted in the network at any point without having to make changes to your network or its components. However, some advanced firewall features are available only in NAT/Route mode.

## VLANs and virtual domains

Fortigate Antivirus Firewalls support IEEE 802.1Q-compliant virtual LAN (VLAN) tags. Using VLAN technology, a single FortiGate unit can provide security services to, and control connections between, multiple security domains according to the VLAN IDs added to VLAN packets. The FortiGate unit can recognize VLAN IDs and apply security policies to secure network and IPSec VPN traffic between each security domain. The FortiGate unit can also apply authentication, content filtering, and antivirus protection to VLAN-tagged network and VPN traffic.

The FortiGate unit supports VLANs in NAT/Route and Transparent mode. In NAT/Route mode, you enter VLAN subinterfaces to receive and send VLAN packets.

FortiGate virtual domains provide multiple logical firewalls and routers in a single FortiGate unit. Using virtual domains, one FortiGate unit can provide exclusive firewall and routing services to multiple networks so that traffic from each network is effectively separated from every other network.

You can develop and manage interfaces, VLAN subinterfaces, zones, firewall policies, routing, and VPN configuration for each virtual domain separately. For these configuration settings, each virtual domain is functionally similar to a single FortiGate unit. This separation simplifies configuration because you do not have to manage as many routes or firewall policies at one time.



## Intrusion Prevention System (IPS)

The FortiGate Intrusion Prevention System (IPS) combines signature and anomaly based intrusion detection and prevention. The FortiGate unit can record suspicious traffic in logs, can send alert email to system administrators, and can log, pass, drop, reset, or clear suspicious packets or sessions. Both the IPS predefined signatures and the IPS engine are upgradeable through the FortiProtect Distribution Network (FDN). You can also create custom signatures.

## VPN

Using FortiGate virtual private networking (VPN), you can provide a secure connection between widely separated office networks or securely link telecommuters or travellers to an office network.

FortiGate VPN features include the following:

- Industry standard and ICSA-certified IPsec VPN, including:
  - IPsec VPN in NAT/Route and Transparent mode,
  - IPsec, ESP security in tunnel mode,
  - DES, 3DES (triple-DES), and AES hardware accelerated encryption,
  - HMAC MD5 and HMAC SHA1 authentication and data integrity,
  - AutoIKE key based on pre-shared key tunnels,
  - IPsec VPN using local or CA certificates,
  - Manual Keys tunnels,
  - Diffie-Hellman groups 1, 2, and 5,
  - Aggressive and Main Mode,
  - Replay Detection,
  - Perfect Forward Secrecy,
  - XAuth authentication,
  - Dead peer detection,
  - DHCP over IPsec,
  - Secure Internet browsing.
- PPTP for easy connectivity with the VPN standard supported by the most popular operating systems.
- L2TP for easy connectivity with a more secure VPN standard, also supported by many popular operating systems.
- Firewall policy based control of IPsec VPN traffic.
- IPsec NAT traversal so that remote IPsec VPN gateways or clients behind a NAT can connect to an IPsec VPN tunnel.
- VPN hub and spoke using a VPN concentrator to allow VPN traffic to pass from one tunnel to another through the FortiGate unit.
- IPsec Redundancy to create a redundant AutoIKE key IPsec VPN connection to a remote network.

## High availability

Fortinet achieves high availability (HA) using redundant hardware and the FortiGate Clustering Protocol (FGCP). Each FortiGate unit in an HA cluster enforces the same overall security policy and shares the same configuration settings. You can add up to 32 FortiGate units to an HA cluster. Each FortiGate unit in an HA cluster must be the same model and must be running the same FortiOS firmware image.

FortiGate HA supports link redundancy and device redundancy.

FortiGate units can be configured to operate in active-passive (A-P) or active-active (A-A) HA mode. Active-active and active-passive clusters can run in either NAT/Route or Transparent mode.

An active-passive (A-P) HA cluster, also referred to as hot standby HA, consists of a primary FortiGate unit that processes traffic, and one or more subordinate FortiGate units. The subordinate FortiGate units are connected to the network and to the primary FortiGate unit but do not process traffic.

Active-active (A-A) HA load balances virus scanning among all the FortiGate units in the cluster. An active-active HA cluster consists of a primary FortiGate unit that processes traffic and one or more secondary units that also process traffic. The primary FortiGate unit uses a load balancing algorithm to distribute virus scanning to all the FortiGate units in the HA cluster.

## Secure installation, configuration, and management

The first time you power on the FortiGate unit, it is already configured with default IP addresses and security policies. Connect to the web-based manager, set the operating mode, and use the Setup wizard to customize FortiGate IP addresses for your network, and the FortiGate unit is ready to protect your network. You can then use the web-based manager to customize advanced FortiGate features.

You can also create a basic configuration using the FortiGate command line interface (CLI).

### Web-based manager

Using HTTP or a secure HTTPS connection from any computer running Internet Explorer, you can configure and manage the FortiGate unit. The web-based manager supports multiple languages. You can configure the FortiGate unit for HTTP and HTTPS administration from any FortiGate interface.

You can use the web-based manager to configure most FortiGate settings. You can also use the web-based manager to monitor the status of the FortiGate unit. Configuration changes made using the web-based manager are effective immediately without resetting the firewall or interrupting service. Once you are satisfied with a configuration, you can download and save it. The saved configuration can be restored at any time.

### Command line interface

You can access the FortiGate command line interface (CLI) by connecting a management computer serial port to the FortiGate RS-232 serial console connector. You can also use Telnet or a secure SSH connection to connect to the CLI from any network that is connected to the FortiGate unit, including the Internet.

The CLI supports the same configuration and monitoring functionality as the web-based manager. In addition, you can use the CLI for advanced configuration options that are not available from the web-based manager.

This *Administration Guide* contains information about basic and advanced CLI commands. For a more complete description about connecting to and using the FortiGate CLI, see the *FortiGate CLI Reference Guide*.

## Logging and reporting

The FortiGate unit supports logging for various categories of traffic and configuration changes. You can configure logging to:

- report traffic that connects to the firewall,
- report network services used,
- report traffic that was permitted by firewall policies,
- report traffic that was denied by firewall policies,
- report events such as configuration changes and other management events, IPSec tunnel negotiation, virus detection, attacks, and web page blocking,
- report attacks detected by the IPS,
- send alert email to system administrators to report virus incidents, intrusions, and firewall or VPN events or violations.

Logs can be sent to a remote syslog server or a WebTrends NetIQ Security Reporting Center and Firewall Suite server using the WebTrends enhanced log format. Some models can also save logs to an optional internal hard drive. If a hard drive is not installed, you can configure most FortiGate units to log the most recent events and attacks detected by the IPS to the system memory.

## Document conventions

This guide uses the following conventions to describe CLI command syntax.

- Angle brackets < > to indicate variables.

For example:

```
execute restore config <filename_str>
```

You enter:

```
execute restore config myfile.bak
```

<xxx\_str> indicates an ASCII string that does not contain new-lines or carriage returns.

<xxx\_integer> indicates an integer string that is a decimal (base 10) number.

<xxx\_octet> indicates a hexadecimal string that uses the digits 0-9 and letters A-F.

<xxx\_ipv4> indicates a dotted decimal IPv4 address.

<xxx\_v4mask> indicates a dotted decimal IPv4 netmask.

<xxx\_ipv4mask> indicates a dotted decimal IPv4 address followed by a dotted decimal IPv4 netmask.

<xxx\_ipv6> indicates a dotted decimal IPv6 address.

<xxx\_v6mask> indicates a dotted decimal IPv6 netmask.

<xxx\_ipv6mask> indicates a dotted decimal IPv6 address followed by a dotted decimal IPv6 netmask.

- Vertical bar and curly brackets { | } to separate alternative, mutually exclusive required keywords.

For example:

```
set opmode {nat | transparent}
```

You can enter `set opmode nat` or `set opmode transparent`.

- Square brackets [ ] to indicate that a keyword or variable is optional.

For example:

```
show system interface [<name_str>]
```

To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the internal interface, you can enter `show system interface internal`.

- A space to separate options that can be entered in any combination and must be separated by spaces.

For example:

```
set allowaccess {ping https ssh snmp http telnet}
```

You can enter any of the following:

```
set allowaccess ping
```

```
set allowaccess ping https ssh
```

```
set allowaccess https ping ssh
```

```
set allowaccess snmp
```

In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.

## FortiGate documentation

Information about FortiGate products is available from the following guides:

- *FortiGate QuickStart Guide*  
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*  
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*  
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*  
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference Guide*  
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference Guide*  
Describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability Guide*  
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS Guide*  
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate VPN Guide*  
Explains how to configure VPNs using the web-based manager.

### Fortinet Knowledge Center

The most recent Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains short how-to articles, FAQs, technical notes, product and feature guides, and much more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

### Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## Related documentation

Additional information about Fortinet products is available from the following related documentation.

### FortiManager documentation

- *FortiManager QuickStart Guide*  
Explains how to install the FortiManager Console, set up the FortiManager Server, and configure basic settings.
- *FortiManager System Administration Guide*  
Describes how to use the FortiManager System to manage FortiGate devices.
- *FortiManager System online help*  
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the FortiManager Console as you work.

### FortiClient documentation

- *FortiClient Host Security User Guide*  
Describes how to use FortiClient Host Security software to set up a VPN connection from your computer to remote networks, scan your computer for viruses, and restrict access to your computer and applications by setting up firewall policies.
- *FortiClient Host Security online help*  
Provides information and procedures for using and configuring the FortiClient software.

### FortiMail documentation

- *FortiMail Administration Guide*  
Describes how to install, configure, and manage a FortiMail unit in gateway mode and server mode, including how to configure the unit; create profiles and policies; configure antispam and antivirus filters; create user accounts; and set up logging and reporting.
- *FortiMail online help*  
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiMail Web Mail Online Help*  
Describes how to use the FortiMail web-based email client, including how to send and receive email; how to add, import, and export addresses; and how to configure message display preferences.

## FortiLog documentation

- *FortiLog Administration Guide*

Describes how to install and configure a FortiLog unit to collect FortiGate and FortiMail log files. It also describes how to view FortiGate and FortiMail log files, generate and view log reports, and use the FortiLog unit as a NAS server.

- *FortiLog online help*

Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

## Customer service and technical support

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet Technical Support web site at <http://support.fortinet.com>.

You can also register Fortinet products and service contracts from <http://support.fortinet.com> and change your registration information at any time.

Technical support is available through email from any of the following addresses. Choose the email address for your region:

**amer\_support@fortinet.com** For customers in the United States, Canada, Mexico, Latin America and South America.

**apac\_support@fortinet.com** For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia.

**eu\_support@fortinet.com** For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East.

For information about our priority support hotline (live support), see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- your name
- your company's name and location
- your email address
- your telephone number
- your support contract number (if applicable)
- the product name and model number
- the product serial number (if applicable)
- the software or firmware version number
- a detailed description of the problem





## System status

You can connect to the web-based manager and view the current system status of the FortiGate unit. The status information that is displayed includes the system status, unit information, system resources, and session log.

This chapter includes:

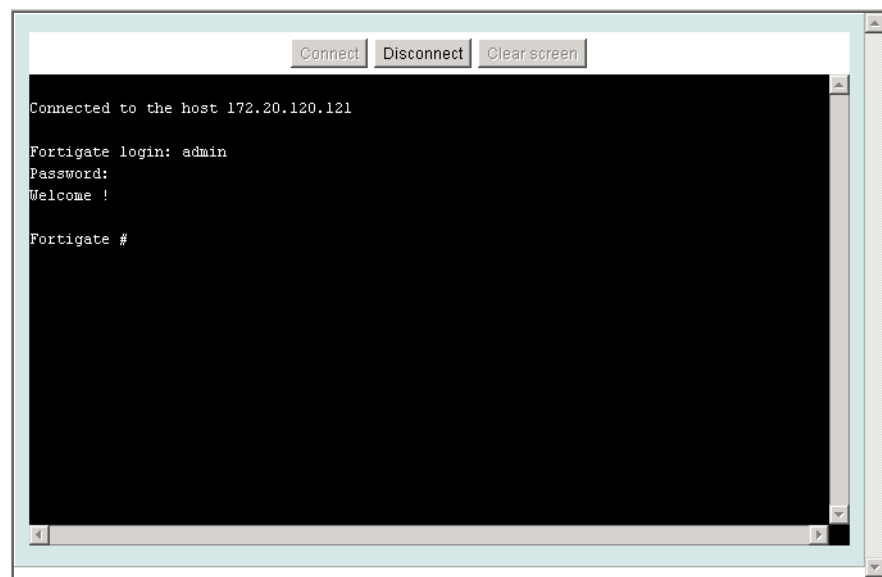
- [Console access](#)
- [Status](#)
- [Session list](#)
- [Changing the FortiGate firmware](#)

### Console access

An alternative to the web-based manager discussed in this manual is text-based Console Access, using the FortiGate command line interface (CLI). You can get console access by selecting Console Access button in the upper right corner of the web-based manager. The management computer must have Java version 1.3 or higher installed.

For information on how to use the CLI, see the *FortiGate CLI Reference Guide*.

**Figure 1: Console access**



- Connect**            Select Connect to connect to the CLI.
- Disconnect**        Select Disconnect to disconnect from the CLI.
- Clear screen**        Select Clear screen to start a new page.

## Status

View the system status page, also known as the system dashboard, for a snap shot of the current operating status of the FortiGate unit. All FortiGate administrators with read access to system configuration can view system status information.

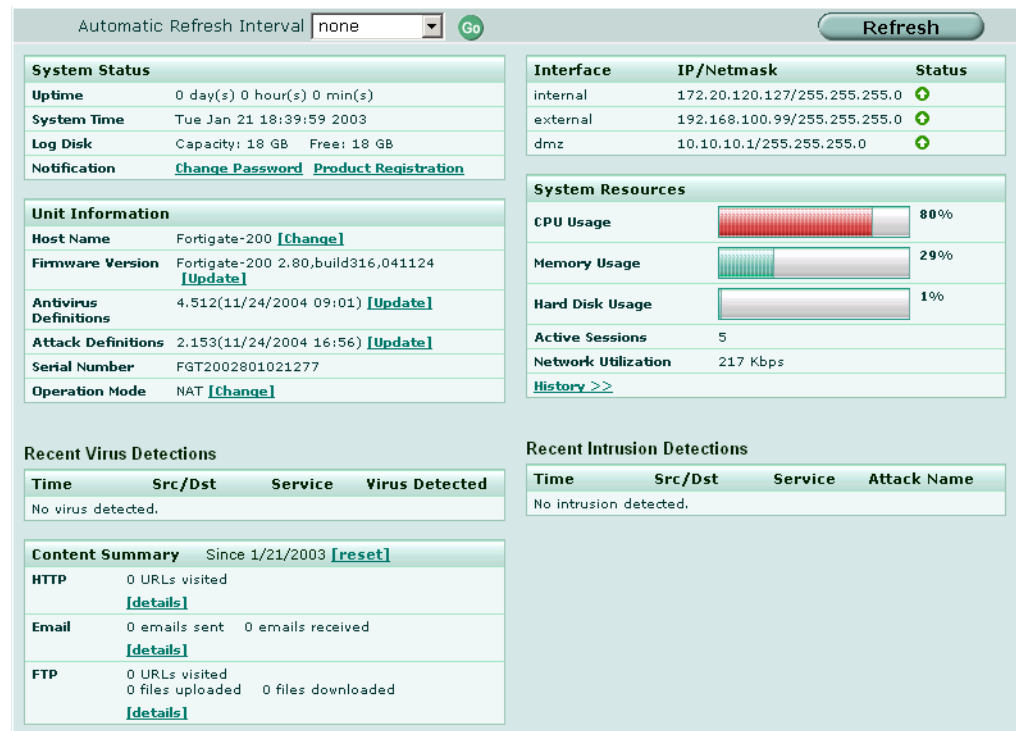
On HA clusters, the Status page shows the status of the primary unit. To view status information for all members of the cluster, go to System > Config > HA and select Cluster Members. For more information, see [“HA configuration” on page 85](#).

FortiGate administrators whose access profiles contain system configuration write privileges can change or update FortiGate unit information. For information on access profiles, see [“Access profiles” on page 111](#).

- [Viewing system status](#)
- [Changing unit information](#)

### Viewing system status

Figure 2: System status



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

## System status

<b>UP Time</b>	The time in days, hours, and minutes since the FortiGate unit was last started.
<b>System Time</b>	The current time according to the FortiGate unit internal clock.
<b>Log Disk</b>	Displays hard disk capacity and free space if the FortiGate unit contains a hard disk or Not Available if no hard disk is installed. The FortiGate unit uses the hard disk to store log messages and quarantine files infected with a virus or blocked by antivirus file blocking.
<b>Notification</b>	Contains reminders such as “Change Password” or “Product Registration”. Select the reminder to see the detailed reminder message.

## Unit Information

Admin users and administrators whose access profiles contain system configuration read and write privileges can change or update the unit information. For information on access profiles, see [“Access profiles” on page 111](#).

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

## Recent Virus Detections

<b>Time</b>	The time at which the recent virus was detected.
<b>Src / Dst</b>	The source and destination addresses of the virus.
<b>Service</b>	The service from which the virus was delivered; HTTP, FTP, IMAP, POP3, or SMTP.
<b>Virus Detected</b>	The name of the virus detected.

## Content Summary

The Content Summary shows information about Content Archiving, configured in firewall protection profiles. The Details pages provide a link to either the FortiLog unit or to the Log & Report > Log Config > Log Setting page where you can configure logging to a FortiLog unit.

---

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

## Interface Status

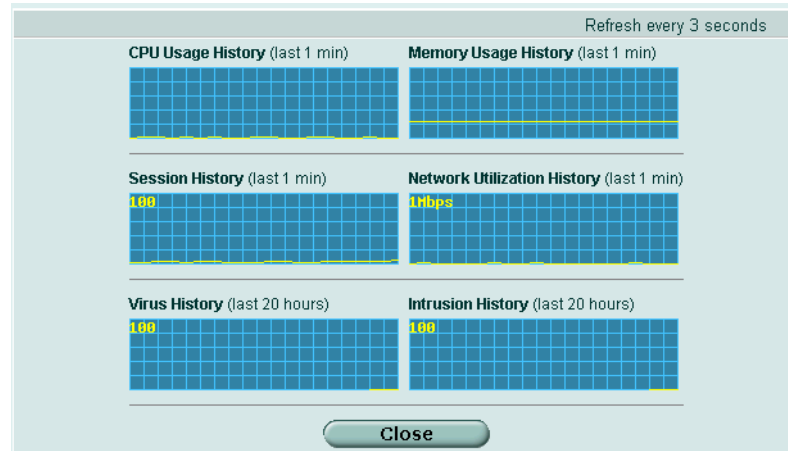
All interfaces in the FortiGate unit are listed in the table.

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

## System Resources

<b>CPU Usage</b>	The current CPU status. The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
<b>Memory Usage</b>	The current memory status. The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
<b>Hard Disk Usage</b>	The current hard disk (local disk) status. The web-based manager displays hard disk usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
<b>Active Sessions</b>	The number of communications sessions being processed by the FortiGate unit.
<b>Network Utilization</b>	The total network bandwidth being used through all FortiGate interfaces and the percentage of the maximum network bandwidth that can be processed by the FortiGate unit.
<b>History</b>	Select History to view a graphical representation of the last minute of CPU, memory, sessions, and network usage. This page also shows the virus and intrusion detections over the last 20 hours.

Figure 3: Sample system resources history



## History

The history page displays 6 graphs representing the following system resources and protection:

<b>CPU Usage History</b>	CPU usage for the previous minute.
<b>Memory Usage History</b>	Memory usage for the previous minute.
<b>Session History</b>	Session history for the previous minute.
<b>Network Utilization History</b>	Network utilization for the previous minute.
<b>Virus History</b>	The virus detection history over the last 20 hours.
<b>Intrusion History</b>	The intrusion detection history over the last 20 hours.

## Recent Intrusion Detections

<b>Time</b>	The time at which the recent intrusion was detected.
<b>Src / Dst</b>	The source and destination addresses of the attack.
<b>Service</b>	The service from which the attack was delivered; HTTP, FTP, IMAP, POP3, or SMTP.
<b>Attack Name</b>	The name of the attack.

## Changing unit information

Administrators with system configuration write access can use the unit information area of the System Status page:

- [To change FortiGate host name](#)
- [To update the firmware version](#)
- [To update the antivirus definitions manually](#)
- [To update the attack definitions manually](#)
- [To change to Transparent mode](#)
- [To change to NAT/Route mode](#)

### To change FortiGate host name

The FortiGate host name appears on the Status page and in the FortiGate CLI prompt. The host name is also used as the SNMP system name. For information about the SNMP system name, see [“SNMP” on page 97](#).

The default host name is FortiGate-200.



**Note:** If the FortiGate unit is part of an HA cluster, you should set a unique name to distinguish the unit from others in the cluster.

- 1 Go to **System > Status > Status**.
  - 2 In the Host Name field of the Unit Information section, select Change.
  - 3 In the New Name field, type a new host name.
  - 4 Select OK.
- The new host name is displayed in the Host Name field, and in the CLI prompt, and is added to the SNMP System Name.

### To update the firmware version

For information on updating the firmware, see [“Changing the FortiGate firmware” on page 33](#).

### To update the antivirus definitions manually



**Note:** For information about configuring the FortiGate unit for automatic antivirus definitions updates, see [“Update center” on page 118](#).

- 1 Download the latest antivirus definitions update file from Fortinet and copy it to the computer that you use to connect to the web-based manager.
- 2 Start the web-based manager and go to **System > Status > Status**.
- 3 In the Antivirus Definitions field of the Unit Information section, select Update.
- 4 In the Update File field, type the path and filename for the antivirus definitions update file, or select Browse and locate the antivirus definitions update file.
- 5 Select OK to copy the antivirus definitions update file to the FortiGate unit.  
The FortiGate unit updates the antivirus definitions. This takes about 1 minute.
- 6 Go to **System > Status** to confirm that the Antivirus Definitions Version information has updated.

### To update the attack definitions manually



**Note:** For information about configuring the FortiGate unit for automatic attack definitions updates, see [“Update center” on page 118](#).

- 1 Download the latest attack definitions update file from Fortinet and copy it to the computer that you use to connect to the web-based manager.
- 2 Start the web-based manager and go to **System > Status > Status**.

- 3 In the Attack Definitions field of the Unit Information section, select Update. The Intrusion Detection System Definitions Update dialog box appears.
- 4 In the Update File field, type the path and filename for the attack definitions update file, or select Browse and locate the attack definitions update file.
- 5 Select OK to copy the attack definitions update file to the FortiGate unit. The FortiGate unit updates the attack definitions. This takes about 1 minute.
- 6 Go to **System > Status > Status** to confirm that the Attack Definitions Version information has updated.

#### To change to Transparent mode

After you change the FortiGate unit from the NAT/Route mode to Transparent mode, most of the configuration resets to Transparent mode factory defaults, except for HA settings (see “HA” on page 84).

- 1 Go to **System > Status > Status**.
- 2 In the Operation Mode field of the Unit Information section, select Change.
- 3 In the Operation Mode field, select Transparent.
- 4 Select OK.  
The FortiGate unit changes operation mode.
- 5 To reconnect to the web-based manager, connect to the interface configured for Transparent mode management access and browse to https:// followed by the Transparent mode management IP address.  
By default in Transparent mode, you can connect to the internal interface. The default Transparent mode management IP address is 10.10.10.1.



**Note:** If the web-based manager IP address was on a different subnet in NAT/Route mode, you may have to change the IP address of your computer to the same subnet as the management IP address.

#### To change to NAT/Route mode

After you change the FortiGate unit from the NAT/Route mode to Transparent mode, most of the configuration resets to Transparent mode factory defaults, except for HA settings (see “HA” on page 84).

- 1 Go to **System > Status > Status**.
- 2 In the Operation Mode field of the Unit Information section, select Change.
- 3 In the Operation Mode field, select NAT/Route.
- 4 Select OK.  
The FortiGate unit changes operation mode.
- 5 To reconnect to the web-based manager, you must connect to the interface configured by default for management access.  
By default in NAT/Route mode, you can connect to the internal interface. The default internal interface IP address is 192.168.1.99.



**Note:** If the management IP address was on a different subnet in Transparent mode, you may have to change the IP address of your computer to the same subnet as the interface configured for management access.

## Session list

The session list displays information about the communications sessions currently being processed by the FortiGate unit. You can use the session list to view current sessions.

**Figure 4: Sample session list**

Protocol	From IP	From Port	To IP	To Port	Expire(secs)
tcp	172.20.120.52	1242	172.20.120.123	443	119
tcp	172.20.120.52	1244	172.20.120.123	443	3599
tcp	172.20.120.52	1243	172.20.120.123	443	3599

<b>From IP</b>	Set source IP address for list filtering
<b>From Port</b>	Set source port for list filtering
<b>To IP</b>	Set destination IP address for list filtering
<b>To Port</b>	Set destination port for list filtering
<b>Apply Filter</b>	Select to filter session list
<b>Virtual Domain</b>	Select a virtual domain to list the sessions being processed by that virtual domain. Select All to view sessions being processed by all virtual domains.
<b>Total Number of Sessions</b>	Total number of sessions currently being conducted through the FortiGate unit.
	Refresh icon. Select to update the session list
	Page up icon. Select to view previous page in the session list
	Page down icon. Select to view the next page in the session list.
<b>Protocol</b>	The service protocol of the connection, for example, udp, tcp, or icmp.
<b>From IP</b>	The source IP address of the connection.
<b>From Port</b>	The source port of the connection.
<b>To IP</b>	The destination IP address of the connection.
<b>To Port</b>	The destination port of the connection.
<b>Expire</b>	The time, in seconds, before the connection expires.
	Delete icon. Select to stop an active communication session.

### To view the session list

- 1 Go to **System > Status > Session**.  
The web-based manager displays the total number of active sessions in the FortiGate unit session table and lists the top 16.
- 2 To navigate the list of sessions, select Page Up or Page Down.
- 3 Select Refresh to update the session list.
- 4 If you are logged in as an administrative user with read and write privileges or as the admin user, you can select Delete to stop an active session.



## Changing the FortiGate firmware

FortiGate administrators whose access profiles contain system configuration read and write privileges and the FortiGate admin user can change the FortiGate firmware.

After you download a FortiGate firmware image from Fortinet, you can use the procedures listed in [Table 1](#) to install the firmware image on your FortiGate unit.

**Table 1: Firmware upgrade procedures**

Procedure	Description
<a href="#">Upgrading to a new firmware version</a>	Use the web-based manager or CLI procedure to upgrade to a new FortiOS firmware version or to a more recent build of the same firmware version.
<a href="#">Reverting to a previous firmware version</a>	Use the web-based manager or CLI procedure to revert to a previous firmware version. This procedure reverts the FortiGate unit to its factory default configuration.
<a href="#">Installing firmware images from a system reboot using the CLI</a>	Use this procedure to install a new firmware version or revert to a previous firmware version. To use this procedure you must connect to the CLI using the FortiGate console port and a null-modem cable. This procedure reverts the FortiGate unit to its factory default configuration.
<a href="#">Testing a new firmware image before installing it</a>	Use this procedure to test a new firmware image before installing it. To use this procedure you must connect to the CLI using the FortiGate console port and a null-modem cable. This procedure temporarily installs a new firmware image using your current configuration. You can test the firmware image before installing it permanently. If the firmware image works correctly you can use one of the other procedures listed in this table to install it permanently.
<a href="#">Installing and using a backup firmware image</a>	If the FortiGate unit is running BIOS version v3.x, you can install a backup firmware image. Once the backup firmware image is installed you can switch to this backup image when required.

### Upgrading to a new firmware version

Use the following procedures to upgrade the FortiGate unit to a newer firmware version.

#### Upgrading the firmware using the web-based manager



**Note:** Installing firmware replaces the current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware, use the procedure [“To update antivirus and attack definitions” on page 120](#) to make sure that antivirus and attack definitions are up to date.

#### To upgrade the firmware using the web-based manager

- 1 Copy the firmware image file to your management computer.
- 2 Log into the web-based manager as the admin administrative user.



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

- 3 Go to **System > Status**.
- 4 Under **Unit Information > Firmware Version**, select Update.
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.  
The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.
- 7 Log into the web-based manager.
- 8 Go to **System > Status** and check the Firmware Version to confirm that the firmware upgrade is successfully installed.
- 9 Update antivirus and attack definitions. For information about updating antivirus and attack definitions, see [“Update center” on page 118](#).


### Upgrading the firmware using the CLI

To use the following procedure you must have a TFTP server that the FortiGate unit can connect to.



**Note:** Installing firmware replaces your current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware, use the procedure [“To update antivirus and attack definitions” on page 120](#) to make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update_now` to update the antivirus and attack definitions.

#### To upgrade the firmware using the CLI

- 1 Make sure that the TFTP server is running.
  - 2 Copy the new firmware image file to the root directory of the TFTP server.
  - 3 Log into the CLI.
-  **Note:** To use this procedure you must login using the admin administrator account, or an administrator account that has system configuration read and write privileges.
- 4 Make sure the FortiGate unit can connect to the TFTP server.  
You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:  

```
execute ping 192.168.1.168
```
  - 5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:  

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

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

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

The FortiGate unit responds with the message:

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

**6** Type `y`.

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

**7** Reconnect to the CLI.

**8** To confirm that the new firmware image is successfully installed, enter:

```
get system status
```

**9** Use the procedure [“To update antivirus and attack definitions” on page 120](#) to update antivirus and attack definitions, or from the CLI, enter:

```
execute update_now
```

## Reverting to a previous firmware version

Use the following procedures to revert your FortiGate unit to a previous firmware version.

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

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

Before beginning this procedure you can:

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

For information, see [“Backing up and Restoring” on page 116](#).

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.80 to FortiOS v2.50), you might not be able to restore the previous configuration from the backup configuration file.



**Note:** Installing firmware replaces the current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware, use the procedure [“To update antivirus and attack definitions” on page 120](#) to make sure that antivirus and attack definitions are up to date.

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

- 1** Copy the firmware image file to the management computer.

- 2 Log into the FortiGate web-based manager.



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

- 3 Go to **System > Status**.
- 4 Under **Unit Information > Firmware Version**, select Update.
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.  
The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.
- 7 Log into the web-based manager.
- 8 Go to **System > Status** and check the Firmware Version to confirm that the firmware is successfully installed.
- 9 Restore your configuration.  
For information about restoring your configuration, see [“Backup and restore” on page 115](#).
- 10 Update antivirus and attack definitions.  
For information about antivirus and attack definitions, see [“To update antivirus and attack definitions” on page 120](#).

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

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

Before beginning this procedure you can:

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

For information, see [“Backing up and Restoring” on page 116](#).

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.80 to FortiOS v2.50), you might not be able to restore your previous configuration from the backup configuration file.



**Note:** Installing firmware replaces the current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware, use the procedure [“To update antivirus and attack definitions” on page 120](#) to make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update_now` to update the antivirus and attack definitions.

To use the following procedure you must have a TFTP server that the FortiGate unit can connect to.

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

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



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

- 4 Make sure the FortiGate unit can connect to the TFTP server.  
You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

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

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

Where <name\_str> is the name of the firmware image file and <tftp\_ip> is the IP address of the TFTP server. For example, if the firmware image file name is FGT\_300-v280-build158-FORTINET.out and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image FGT_300-v280-build158-FORTINET.out  
192.168.1.168
```

The FortiGate unit responds with the message:

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

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

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

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

- 8 Reconnect to the CLI.
- 9 To confirm that the new firmware image has been loaded, enter:

```
get system status
```

- 10 To restore your previous configuration if needed, use the command:

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

**11** Update antivirus and attack definitions.

For information, see [“To update antivirus and attack definitions” on page 120](#), or from the CLI, enter:

```
execute update_now
```

## Installing firmware images from a system reboot using the CLI

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



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

For this procedure you:

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

Before beginning this procedure you can:

- Back up the FortiGate unit configuration.  
For information, see [“Backing up and Restoring” on page 116](#).
- Back up the IPS custom signatures.  
For information, see [“Backing up and restoring custom signature files” on page 283](#).
- Back up web content and email filtering lists.  
For information, see [“Web filter” on page 309](#) and [“Spam filter” on page 323](#).

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.80 to FortiOS v2.50), you might not be able to restore your previous configuration from the backup configuration file.



**Note:** Installing firmware replaces the current antivirus and attack definitions with the definitions included with the firmware release that you are installing. After you install new firmware, use the procedure [“To update antivirus and attack definitions” on page 120](#) to make sure that antivirus and attack definitions are up to date.

### To install firmware from a system reboot

- 1 Connect to the CLI using the null-modem cable and FortiGate console port.
- 2 Make sure that the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of the TFTP server.
- 4 Make sure that the internal interface is connected to the same network as the TFTP server.

- 5 To confirm that the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168, enter:

```
execute ping 192.168.1.168
```

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

```
execute reboot
```

The FortiGate unit responds with the following message:

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

- 7 Type `y`.

As the FortiGate units starts, a series of system startup messages is displayed.

When one of the following messages appears:

- FortiGate unit running v2.x BIOS  
Press Any Key To Download Boot Image.  
...
- FortiGate unit running v3.x BIOS  
Press any key to display configuration menu.....  
.....

Immediately press any key to interrupt the system startup.



**Note:** You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

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

- FortiGate unit running v2.x BIOS  
Enter TFTP Server Address [192.168.1.168]:  
Go to step 9.
- FortiGate unit running v3.x BIOS  
[G]: Get firmware image from TFTP server.  
[F]: Format boot device.  
[B]: Boot with backup firmware and set as default.  
[Q]: Quit menu and continue to boot with default firmware.  
[H]: Display this list of options.

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

- 8 Type `G` to get the new firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

- 9 Type the address of the TFTP server and press `Enter`.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

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

## Restoring the previous configuration

Change the internal interface address if required. You can do this from the CLI using the command:

```
config system interface
  edit internal
    set ip <address_ipv4mask>
    set allowaccess {ping https ssh telnet http}
  end
```

After changing the interface address, you can access the FortiGate unit from the web-based manager and restore the configuration.

- To restore the FortiGate unit configuration, see [“Backup and restore” on page 115](#).
- To restore IPS custom signatures, see [“Backing up and restoring custom signature files” on page 283](#).
- To restore web content filtering lists, see [“Backup and restore” on page 115](#).
- To restore email filtering lists, see [“Backup and restore” on page 115](#).
- To update the virus and attack definitions to the most recent version, see [“Updating antivirus and attack definitions” on page 120](#).

If you are reverting to a previous firmware version (for example, reverting from FortiOS v2.80 to FortiOS v2.50), you might not be able to restore your previous configuration from the backup up configuration file.



## Testing a new firmware image before installing it

You can test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure the FortiGate unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure [“Upgrading to a new firmware version” on page 33](#).

For this procedure you:

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

### To test a new firmware image

- 1 Connect to the CLI using a null-modem cable and FortiGate console port.
- 2 Make sure the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of the TFTP server.
- 4 Make sure that the internal interface is connected to the same network as the TFTP server.

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

```
execute ping 192.168.1.168
```

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

```
execute reboot
```

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

- FortiGate unit running v2.x BIOS  
Press Any Key To Download Boot Image.  
...
- FortiGate unit running v3.x BIOS  
Press any key to display configuration menu.....  
.....

- 7 Immediately press any key to interrupt the system startup.



**Note:** You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

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

- FortiGate unit running v2.x BIOS

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

Go to step 9.

- FortiGate unit running v3.x BIOS

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

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

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

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

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

- 8 Type G to get the new firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

- 9 Type the address of the TFTP server and press Enter.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

- 10 Type an IP address that can be used by the FortiGate unit to connect to the FTP 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 this network.

The following message appears:

```
Enter File Name [image.out]:
```

- 11 Enter the firmware image file name and press Enter.

The TFTP server uploads the firmware image file to the FortiGate unit and messages similar to the following appear.

- FortiGate unit running v2.x BIOS

```
Do You Want To Save The Image? [Y/n]
```

Type N.

- FortiGate unit running v3.x BIOS

```
Save as Default firmware/Run image without saving:[D/R]
```

or

```
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
```

- 12 Type R.

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

- 13 You can log into the CLI or the web-based manager using any administrative account.

- 14 To confirm that the new firmware image has been loaded, from the CLI enter:

```
get system status
```

You can test the new firmware image as required.

## Installing and using a backup firmware image

If the FortiGate unit is running BIOS version v3.x, you can install a backup firmware image. Once the backup firmware image is installed you can switch to this backup image when required.

- [Installing a backup firmware image](#)
- [Switching to the backup firmware image](#)
- [Switching back to the default firmware image](#)

### Installing a backup firmware image

To run this procedure you:

- access the CLI by connecting to the FortiGate console port using a null-modem cable,
- install a TFTP server that you can connect to from the FortiGate as described in the procedure “[Installing firmware images from a system reboot using the CLI](#)” on [page 38](#).

#### To install a backup firmware image

- 1 Connect to the CLI using the null-modem cable and FortiGate console port.
- 2 Make sure that the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of your TFTP server.
- 4 To confirm that the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:
 

```
execute ping 192.168.1.168
```
- 5 Enter the following command to restart the FortiGate unit:
 

```
execute reboot
```

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

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



**Note:** You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

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

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

Enter G, F, B, 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 [192.168.1.188]:
- 9 Type an IP address that can be used by the FortiGate unit to connect to the FTP server.  
The IP address can be any IP address that is valid for the network that the interface is connected to. Make sure you do not enter the IP address of another device on this 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 message is displayed.  
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]
- 11 Type B.  
The FortiGate unit saves the backup firmware image and restarts. When the FortiGate unit restarts it is running the previously installed firmware version.

### Switching to the backup firmware image

Use this procedure to switch the FortiGate unit to operating with a backup firmware image that you previously installed. When you switch the FortiGate unit to the backup firmware image, the FortiGate unit operates using the configuration that was saved with that firmware image.

If you install a new backup image from a reboot, the configuration saved with this firmware image is the factory default configuration. If you use the procedure [“Switching back to the default firmware image” on page 45](#) to switch to a backup firmware image that was previously running as the default firmware image, the configuration saved with this firmware image is restored.

#### To switch to the backup firmware image

- 1 Connect to the CLI using the null-modem cable and FortiGate console port.
- 2 Enter the following command to restart the FortiGate unit:  

```
execute reboot
```

As the FortiGate units starts, a series of system startup messages are displayed. When the following message appears:  
Press any key to enter configuration menu.....  
.....
- 3 Immediately press any key to interrupt the system startup.



**Note:** You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

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

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

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

- 4 Type B to load the backup firmware image.

The FortiGate unit loads the backup firmware image and restarts. When the FortiGate unit restarts, it is running the backup firmware version and the configuration is set to factory default.

### Switching back to the default firmware image

Use this procedure to switch the FortiGate unit to operating with the backup firmware image that had been running as the default firmware image. When you switch to this backup firmware image, the configuration saved with this firmware image is restored.

#### To switch back to the default firmware image

- 1 Connect to the CLI using the null-modem cable and FortiGate console port.
- 2 Enter the following command to restart the FortiGate unit:

```
execute reboot
```

As the FortiGate unit starts, a series of system startup messages are displayed.

When the following message appears:

```
Press any key to enter configuration menu.....
.....
```

- 3 Immediately press any key to interrupt the system startup.



**Note:** You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

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

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

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

- 4 Type B to load the backup firmware image.

The FortiGate unit loads the backup firmware image and restarts. When the FortiGate unit restarts it is running the backup firmware version with a restored configuration.



## System network

System network settings control how the FortiGate unit connects to and interacts with your network. Basic network settings start with configuring FortiGate interfaces to connect to your network and configuring the FortiGate DNS settings.

More advanced network settings include adding VLAN subinterfaces and zones to the FortiGate network configuration.

- [Interface](#)
- [Zone](#)
- [Management](#)
- [DNS](#)
- [Routing table \(Transparent Mode\)](#)
- [VLAN overview](#)
- [VLANs in NAT/Route mode](#)
- [VLANs in Transparent mode](#)
- [FortiGate IPv6 support](#)

## Interface

In NAT/Route mode, go to **System > Network > Interface** to configure FortiGate interfaces and to add and configure VLAN subinterfaces.



**Note:** Unless stated otherwise, in this section the term interface can refer to a physical FortiGate interface or to a FortiGate VLAN subinterface.

- For information about VLANs in NAT/Route mode, see “[VLANs in NAT/Route mode](#)” on page 63.
- For information about VLANs in Transparent mode, see “[VLANs in Transparent mode](#)” on page 66.

**Figure 5: Interface list**

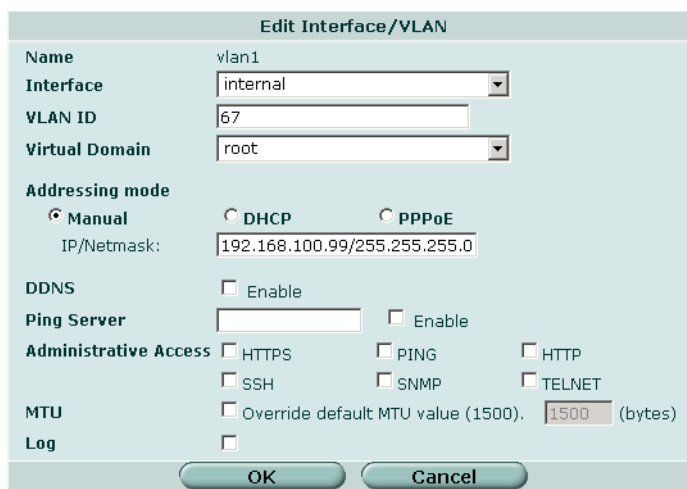
Create New		Virtual Domain: All			
Name	IP	Netmask	Access	Status	
internal	172.20.120.125	255.255.255.0	HTTPS,PING,SSH	Bring Down	
external	64.63.62.61	255.255.255.0	HTTPS,PING	Bring Down	
dmz	10.10.10.1	255.255.255.0	HTTPS,PING	Bring Down	

<b>Create New</b>	Select Create New to create a VLAN.
<b>Virtual Domain</b>	Select a virtual domain to display the interfaces added to this virtual domain. Only available if you have added a virtual domain.
<b>Name</b>	The names of the physical interfaces available to your FortiGate unit. <ul style="list-style-type: none"><li>• Interface names indicate the default function of the interface (for example, internal and external)</li></ul> If you have added VLAN subinterfaces, they also appear in the name list, below the physical interface that they have been added to. See <a href="#">“VLAN overview” on page 62</a> .
<b>IP</b>	The current IP address of the interface.
<b>Netmask</b>	The netmask of the interface.
<b>Access</b>	The administrative access configuration for the interface. See <a href="#">“To control administrative access to an interface” on page 57</a> for information about administrative access options.
<b>Status</b>	The administrative status for the interface. If the administrative status is a green arrow, the interface is up and can accept network traffic. If the administrative status is a red arrow, the interface is administratively down and cannot accept traffic. To change the administrative status, select Bring Down or Bring Up. For more information, see <a href="#">“To bring down an interface that is administratively up” on page 54</a> and <a href="#">“To start up an interface that is administratively down” on page 54</a> . Delete, edit, and view icons.

## Interface settings

Interface settings displays the current configuration of a selected FortiGate interface or VLAN subinterface. Use interface settings to configure a new VLAN subinterface or to change the configuration of a FortiGate interface or VLAN subinterface.

Figure 6: Interface settings





See the following procedures for configuring interfaces:

- [To bring down an interface that is administratively up](#)
- [To start up an interface that is administratively down](#)
- [To add interfaces to a zone](#)
- [To add an interface to a virtual domain](#)
- [To change the static IP address of an interface](#)
- [To configure an interface for DHCP](#)
- [To configure an interface for PPPoE](#)
- [To configure support for dynamic DNS services](#)
- [To add a secondary IP address](#)
- [To add a ping server to an interface](#)
- [To control administrative access to an interface](#)
- [To change the MTU size of the packets leaving an interface](#)
- [To configure traffic logging for connections to an interface](#)

### Name

The name of the Interface.

### Interface

Select the name of the physical interface to add the VLAN subinterface to. All VLAN subinterfaces must be associated with a physical interface. Once created, the VLAN is listed below its physical interface in the Interface list.

### VLAN ID

Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface. You cannot change the VLAN ID of an existing VLAN subinterface.

The VLAN ID can be any number between 1 and 4096 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch connected to the VLAN subinterface.

For more information on VLANs, see [“VLAN overview” on page 62](#).

### Virtual Domain

Select a virtual domain to add the interface or VLAN subinterface to this virtual domain. Virtual domain is only available if you have added a virtual domain.

For more information on virtual domains, see [“System virtual domain” on page 131](#).

### Addressing mode

Select Manual, DHCP, or PPPoE to set the addressing mode for this interface.

## Manual

Select Manual and enter an IP address and netmask for the interface. The IP address of the interface must be on the same subnet as the network the interface is connecting to.



**Note:** Where you can enter both an IP address and a netmask in the same field, you can use the short form of the netmask. For example, 192.168.1.100/255.255.255.0 can also be entered as 192.168.1.100/24.

Two interfaces cannot have the same IP address and cannot have IP addresses on the same subnet.

## DHCP

If you configure the interface to use DHCP, the FortiGate unit automatically broadcasts a DHCP request. You can disable Connect to server if you are configuring the FortiGate unit offline and you do not want the FortiGate unit to send the DHCP request.

<b>Distance</b>	Enter the administrative distance for the default gateway retrieved from the DHCP server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. The default distance for the default gateway is 1.
<b>Retrieve default gateway from server</b>	Enable Retrieve default gateway from server to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table.
<b>Override internal DNS</b>	Enable Override internal DNS to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page.
<b>Connect to server</b>	Enable Connect to Server so that the interface automatically attempts to connect to a DHCP server. Disable this option if you are configuring the interface offline.
<b>Status</b>	Displays DHCP status messages as the FortiGate unit connects to the DHCP server and gets addressing information. Select Status to refresh the addressing mode status message.
<b>initializing</b>	No activity.
<b>connecting</b>	The interface is attempting to connect to the DHCP server.
<b>connected</b>	The interface retrieves an IP address, netmask, and other settings from the DHCP server.
<b>failed</b>	The interface was unable to retrieve an IP address and other information from the DHCP server.

## PPPoE

If you configure the interface to use PPPoE, the FortiGate unit automatically broadcasts a PPPoE request. You can disable connect to server if you are configuring the FortiGate unit offline and you do not want the FortiGate unit to send the PPPoE request.

FortiGate units support many of the PPPoE RFC features (RFC 2516) including unnumbered IPs, initial discovery timeout that times and PPPoE Active Discovery Terminate (PADT).

**Figure 7: PPPoE settings**

<b>User Name</b>	The PPPoE account user name.
<b>Password</b>	The PPPoE account password.
<b>Unnumbered IP</b>	Specify the IP address for the interface. If your ISP has assigned you a block of IP addresses, use one of them. Otherwise, this IP address can be the same as the IP address of another interface or can be any IP address.
<b>Initial Disc Timeout</b>	Initial discovery timeout. The time to wait before retrying to start a PPPoE discovery. Set Initial Disc to 0 to disable.
<b>Initial PADT timeout</b>	Initial PPPoE Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP. Set initial PADT timeout to 0 to disable.
<b>Distance</b>	Enter the administrative distance for the default gateway retrieved from the PPPoE server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. The default distance for the default gateway is 1.
<b>Retrieve default gateway from server</b>	Enable Retrieve default gateway from server to retrieve a default gateway IP address from a PPPoE server. The default gateway is added to the static routing table.
<b>Override internal DNS</b>	Enable Override internal DNS to replace the DNS server IP addresses on the DNS page with the DNS addresses retrieved from the PPPoE server.
<b>Connect to server</b>	Enable Connect to Server so that the interface automatically attempts to connect to a PPPoE server. Disable this option if you are configuring the interface offline.
<b>Status</b>	Displays PPPoE status messages as the FortiGate unit connects to the PPPoE server and gets addressing information. Select Status to refresh the addressing mode status message.
<b>initializing</b>	No activity.
<b>connecting</b>	The interface is attempting to connect to the PPPoE server.
<b>connected</b>	The interface retrieves an IP address, netmask, and other settings from the PPPoE server.
<b>failed</b>	The interface was unable to retrieve an IP address and other information from the PPPoE server.

## DDNS

Enable or disable updates to a Dynamic DNS (DDNS) service. When the FortiGate unit has a static domain name and a dynamic public IP address, select DDNS Enable to force the unit to update the DDNS server each time the address changes. In turn, the DDNS service updates Internet DNS servers with the new IP address for the domain.

Dynamic DNS is available only in NAT/Route mode.

- Server** Select a DDNS server to use. The client software for these services is built into the FortiGate firmware. The FortiGate unit can only connect automatically to a DDNS server for the supported clients.
- Domain** The domain name to use for the DDNS service.
- Username** The user name to use when connecting to the DDNS server.
- Password** The password to use when connecting to the DDNS server.

## Ping server

Add a ping server to an interface if you want the FortiGate unit to confirm connectivity with the next hop router on the network connected to the interface. Adding a ping server is required for routing failover. See [“To add or edit a static route” on page 144](#).

The FortiGate unit uses dead gateway detection to ping the Ping Server IP address to make sure that the FortiGate unit can connect to this IP address. To configure dead gateway detection, see [“To modify the dead gateway detection settings” on page 84](#).

## Administrative access

Configure administrative access to an interface to control how administrators access the FortiGate unit and the FortiGate interfaces to which administrators can connect. You can select the following administrative access options:

- HTTPS** To allow secure HTTPS connections to the web-based manager through this interface.
- PING** If you want this interface to respond to pings. Use this setting to verify your installation and for testing.
- HTTP** To allow HTTP connections to the web-based manager through this interface. HTTP connections are not secure and can be intercepted by a third party.
- SSH** To allow SSH connections to the CLI through this interface.
- SNMP** To allow a remote SNMP manager to request SNMP information by connecting to this interface. See [“Configuring SNMP” on page 97](#).
- TELNET** To allow Telnet connections to the CLI through this interface. Telnet connections are not secure and can be intercepted by a third party.

## MTU

To improve network performance, you can change the maximum transmission unit (MTU) of the packets that the FortiGate unit transmits from any interface. Ideally, this MTU should be the same as the smallest MTU of all the networks between the FortiGate unit and the destination of the packets. If the packets that the FortiGate unit sends are larger, they are broken up or fragmented, which slows down transmission. Experiment by lowering the MTU to find an MTU size for best network performance.

To change the MTU, select Override default MTU value (1500) and enter the maximum packet size. For manual and DHCP addressing mode the MTU size can be from 576 to 1500 bytes. For PPPoE addressing mode the MTU size can be from 576 to 1492 bytes.



**Note:** In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces to match the new MTU.

## Log

Select Log to record logs for any traffic to or from the interface. To record logs you must also enable traffic log for a logging location and set the logging severity level to Notification or lower. Go to **Log & Report > Log Config** to configure logging locations and types. For information about logging see “[Log & Report](#)” on page 339.

## Configuring interfaces

Use the following procedures to configure FortiGate interfaces and VLAN subinterfaces.

- [To bring down an interface that is administratively up](#)
- [To add interfaces to a zone](#)
- [To add an interface to a virtual domain](#)
- [To change the static IP address of an interface](#)
- [To configure an interface for DHCP](#)
- [To configure an interface for PPPoE](#)
- [To add a secondary IP address](#)
- [To configure support for dynamic DNS services](#)
- [To add a ping server to an interface](#)
- [To control administrative access to an interface](#)
- [To change the MTU size of the packets leaving an interface](#)
- [To configure traffic logging for connections to an interface](#)

### To add a VLAN subinterface

See “[To add a VLAN subinterface in NAT/Route mode](#)” on page 65.

**To bring down an interface that is administratively up**

You can bring down physical interfaces or VLAN subinterfaces. Bringing down a physical interface also brings down the VLAN subinterfaces associated with it.

- 1 Go to **System > Network > Interface**.  
The interface list is displayed.
- 2 Select Bring Down for the interface that you want to stop.

**To start up an interface that is administratively down**

You can start up physical interfaces and VLAN subinterfaces. Starting a physical interface does not start the VLAN subinterfaces added to it.

- 1 Go to **System > Network > Interface**.  
The interface list is displayed.
- 2 Select Bring Up for the interface that you want to start.

**To add interfaces to a zone**

If you have added zones to the FortiGate unit, you can use this procedure to add interfaces or VLAN subinterfaces to the zone. To add a zone, see [“To add a zone” on page 59](#). You cannot add an interface to a zone if you have added firewall policies for the interface. Delete firewall policies for the interface and then add the interface to the zone.

- 1 Go to **System > Network > Zone**.
- 2 Choose the zone to add the interface or VLAN subinterface to and select Edit.
- 3 Select the names of the interfaces or VLAN subinterfaces to add to the zone.
- 4 Select OK to save the changes.

**To add an interface to a virtual domain**

If you have added virtual domains to the FortiGate unit, you can use this procedure to add an interface or VLAN subinterface to a virtual domain. To add a virtual domain, see [“To add a virtual domain” on page 135](#). You cannot add an interface to a virtual domain if you have added firewall policies for the interface. Delete firewall policies for the interface and then add the interface to the virtual domain.

- 1 Go to **System > Network > Interface**.
- 2 Choose the interface or VLAN subinterface to add to a virtual domain and select Edit.
- 3 From the Virtual Domain list, select the virtual domain that you want to add the interface to.
- 4 Select OK to save the changes.
- 5 Repeat these steps to add more interfaces or VLAN subinterfaces to virtual domains.

**To change the static IP address of an interface**

You can change the static IP address of any FortiGate interface.

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface and select Edit.

- 3 Set Addressing Mode to Manual.
- 4 Change the IP address and Netmask as required.
- 5 Select OK to save your changes.  
If you changed the IP address of the interface to which you are connecting to manage the FortiGate unit, you must reconnect to the web-based manager using the new interface IP address.

#### To configure an interface for DHCP

You can configure any FortiGate interface to use DHCP.

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface and select Edit.
- 3 In the Addressing Mode section, select DHCP.
- 4 Select the Retrieve default gateway and DNS from server check box if you want the FortiGate unit to obtain a default gateway IP address and DNS server IP addresses from the DHCP server.
- 5 Select the Connect to Server check box if you want the FortiGate unit to connect to the DHCP server.
- 6 Select Apply.  
The FortiGate unit attempts to contact the DHCP server from the interface to set the IP address, netmask, and optionally the default gateway IP address, and DNS server IP addresses.
- 7 Select Status to refresh the addressing mode status message.
- 8 Select OK.

#### To configure an interface for PPPoE

Use this procedure to configure any FortiGate interface to use PPPoE. See ["PPPoE" on page 50](#) for information on PPPoE settings.

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface and select Edit.
- 3 In the Addressing Mode section, select PPPoE.
- 4 Enter your PPPoE account User Name and Password.
- 5 Enter an Unnumbered IP if required by your PPPoE service.
- 6 Set the Initial Disc Timeout and Initial PADT Timeout if supported by your ISP.
- 7 Select the Retrieve default gateway from server check box if you want the FortiGate unit to obtain a default gateway IP address from the PPPoE server.
- 8 Select the Override Internal DNS check box if you want the FortiGate unit to obtain a DNS server IP address from the PPPoE server.
- 9 Select the Connect to Server check box if you want the FortiGate unit to connect to the PPPoE server.

- 10 Select Apply.  
The FortiGate unit attempts to contact the PPPoE server from the interface to set the IP address, netmask, and optionally default gateway IP address and DNS server IP addresses.
- 11 Select Status to refresh the addressing mode status message.
- 12 Select OK.

#### To add a secondary IP address

You can use the CLI to add a secondary IP address to any FortiGate interface. The secondary IP address cannot be the same as the primary IP address but it can be on the same subnet.

From the FortiGate CLI, enter the following commands:

```
config system interface
edit <intf_str>
config secondaryip
edit 0
set ip <second_ip> <netmask_ip>
```

Optionally, you can also configure management access and add a ping server to the secondary IP address:

```
set allowaccess ping https ssh snmp http telnet
set gwdetect enable
```

Save the changes:

```
end
```

#### To configure support for dynamic DNS services

- 1 Go to **System > Network > Interface**.
- 2 Select the interface to the Internet and then select Edit.
- 3 Select DDNS Enable.
- 4 From the Server list, select one of the supported dynamic DNS services.
- 5 In the Domain field, type the fully qualified domain name of the FortiGate unit.
- 6 In the Username field, type the user name that the FortiGate unit must send when it connects to the dynamic DNS server.
- 7 In the Password field, type the associated password.
- 8 Select OK.

#### To add a ping server to an interface

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface and select Edit.
- 3 Set Ping Server to the IP address of the next hop router on the network connected to the interface.
- 4 Select the Enable check box.



- 5 Select OK to save the changes.

### To control administrative access to an interface

For a FortiGate unit running in NAT/Route mode, you can control administrative access to an interface to control how administrators access the FortiGate unit and the FortiGate interfaces to which administrators can connect.

Controlling administrative access for an interface connected to the Internet allows remote administration of the FortiGate unit from any location on the Internet. However, allowing remote administration from the Internet could compromise the security of your FortiGate unit. You should avoid allowing administrative access for an interface connected to the Internet unless this is required for your configuration. To improve the security of a FortiGate unit that allows remote administration from the Internet:

- Use secure administrative user passwords,
- Change these passwords regularly,
- Enable secure administrative access to this interface using only HTTPS or SSH,
- Do not change the system idle timeout from the default value of 5 minutes (see [“To set the system idle timeout” on page 83](#)).

To configure administrative access in Transparent mode, see [“To configure the management interface” on page 60](#).

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface and select Edit.
- 3 Select the Administrative Access methods for the interface.
- 4 Select OK to save the changes.

### To change the MTU size of the packets leaving an interface

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface and select Edit.
- 3 Select Override default MTU value (1500).
- 4 Set the MTU size.



**Note:** You cannot set the MTU of a VLAN larger than the MTU of its physical interface. Nor can you set the MTU of a physical interface smaller than the MTU of any VLAN on that interface.

### To configure traffic logging for connections to an interface

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface and select Edit.
- 3 Select the Log check box to record log messages whenever a firewall policy accepts a connection to this interface.
- 4 Select OK to save the changes.

## Zone

You can use zones to group related interfaces and VLAN subinterfaces. Grouping interfaces and VLAN subinterfaces into zones simplifies policy creation. If you group interfaces and VLAN subinterfaces into a zone, you can configure policies for connections to and from this zone, rather than to and from each interface and VLAN subinterface.

You can add zones, rename and edit zones, and delete zones from the zone list. When you add a zone, you select the names of the interfaces and VLAN subinterfaces to add to the zone.

Zones are added to virtual domains. If you have added multiple virtual domains to your FortiGate configuration, make sure you are configuring the correct virtual domain before adding or editing zones.

**Figure 8: Zone list**

Create New			
Name	Block intra-zone traffic	Interface Members	
Zone1	No	internal	
Zone2	Yes	port2, port4	
Zone3	Yes	port6, port8	

- Create New** Select Create New to create a zone.
- Name** The names of the zones that you have added.
- Block intra-zone traffic** Displays Yes if traffic between interfaces in the same zone is blocked and No if traffic between interfaces in the same zone is not blocked.
- Interface Members** The names of the interfaces added to the zone.
- Edit/View icons. Select to edit or view a zone.
- Delete icon. Select to remove a zone.

## Zone settings

**Figure 9: Zone options**

**New Zone**

Zone Name:

Block intra-zone traffic.

**Interface members**

external       dmz

ha                 port1

port3             port5

port7             vlan1

- Name** Enter the name to identify the zone.
- Block intra-zone traffic** Select Block intra-zone traffic to block traffic between interfaces or VLAN subinterfaces in the same zone.
- Interface members** Enable check boxes to select the interfaces that are part of this zone.

**To add a zone**

- 1 If you have added a virtual domain, go to **System > Virtual Domain > Current Virtual Domain** and select the virtual domain to which you want to add the zone.
- 2 Go to **System > Network > Zone**.
- 3 Select Create New.
- 4 In the New Zone dialog box, type a name for the zone.
- 5 Select the Block intra-zone traffic check box if you want to block traffic between interfaces or VLAN subinterfaces in the same zone.
- 6 Select the names of the interfaces or VLAN subinterfaces to add to the zone.
- 7 Select OK.

**To delete a zone**

You can only delete zones that have the Delete icon beside them in the zone list.

- 1 If you have added a virtual domain, go to **System > Virtual Domain > Current Virtual Domain** and select the virtual domain from which to delete the zone.
- 2 Go to **System > Network > Zone**.
- 3 Select Delete to remove a zone from the list.
- 4 Select OK to delete the zone.

**To edit a zone**

- 1 If you have added a virtual domain, go to **System > Virtual Domain > Current Virtual Domain** and select the virtual domain in which to edit the zone.
- 2 Go to **System > Network > Zone**.
- 3 Select Edit to modify a zone.
- 4 Select or deselect Block intra-zone traffic.
- 5 Select the names of the interfaces or VLAN subinterfaces to add to the zone.
- 6 Clear the check box for the names of the interfaces or VLAN subinterfaces to remove from the zone.
- 7 Select OK.

## Management

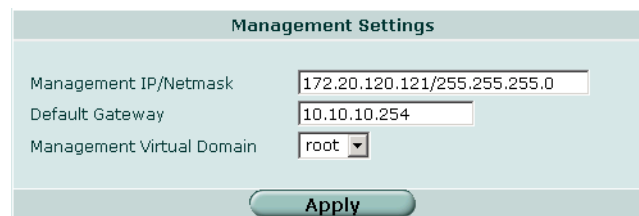
Configure the management interface in Transparent mode to set the management IP address of the FortiGate unit. Administrators connect to this IP address to administer the FortiGate unit. The FortiGate also uses this IP address to connect to the FDN for virus and attack updates (see [“Update center” on page 118](#)).

You can also configure interfaces to control how administrators connect to the FortiGate unit for administration. See [“To control administrative access to an interface” on page 57](#).

Controlling administrative access to a FortiGate interface connected to the Internet allows remote administration of the FortiGate unit from any location on the Internet. However, allowing remote administration from the Internet could compromise the security of the FortiGate unit. You should avoid allowing administrative access for an interface connected to the Internet unless this is required for your configuration. To improve the security of a FortiGate unit that allows remote administration from the Internet:

- Use secure administrative user passwords,
- Change these passwords regularly,
- Enable secure administrative access to this interface using only HTTPS or SSH,
- Do not change the system idle timeout from the default value of 5 minutes (see [“To set the system idle timeout” on page 83](#)).

**Figure 10: Management**



Management Settings	
Management IP/Netmask	172.20.120.121/255.255.255.0
Default Gateway	10.10.10.254
Management Virtual Domain	root
<b>Apply</b>	

- Management IP/Netmask** Enter the management IP address and netmask. This must be a valid IP address for the network that you want to manage the FortiGate unit from.
- Default Gateway** Enter the default gateway address.
- Management Virtual Domain** Select the virtual domain from which you want to perform system management.

### To configure the management interface

- 1 Go to **System > Network > Management**.
- 2 Enter the Management IP/Netmask.
- 3 Enter the Default Gateway.
- 4 Select the Management Virtual Domain.
- 5 Select Apply.  
The FortiGate unit displays the following message:  
Management IP address was changed. [Click here to redirect.](#)
- 6 Click on the message to connect to the new Management IP.

## DNS

Several FortiGate functions, including Alert E-mail and URL blocking, use DNS. You can add the IP addresses of the DNS servers to which your FortiGate unit can connect. DNS server IP addresses are usually supplied by your ISP.

**Figure 11: DNS**

DNS Settings	
Primary DNS Server	207.194.200.1
Second DNS Server	207.194.200.129
Apply	

**Primary DNS Server** Enter the primary DNS server IP address.

**Secondary DNS Server** Enter the secondary DNS server IP address.

### To add DNS server IP addresses

- 1 Go to **System > Network > DNS**.
- 2 Change the primary and secondary DNS server IP addresses as required.
- 3 Select Apply to save the changes.

## Routing table (Transparent Mode)

In Transparent mode, you can configure routing to add static routes from the FortiGate unit to local routers.

### Routing table list

**Figure 12: Routing table**

Create New					
#	IP	Mask	Gateway	Distance	
1	0.0.0.0	0.0.0.0	10.10.10.254	10	

**Create New** Select Create New to add a new route.

**#** Route number.

**IP** The destination IP address for this route.

**Mask** The netmask for this route.

**Gateway** The IP address of the next hop router to which this route directs traffic.

**Distance** The the relative preferability of this route. 1 is most preferred.

Delete icon. Select to remove a route.

View/edit icon. Select to view or edit a route.

Move To icon. Select to change the order of a route in the list.

## Transparent mode route settings

Figure 13: Transparent mode route options

Edit Static Route	
Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Gateway	<input type="text" value="10.10.10.254"/>
Distance	<input type="text" value="10"/> (1-255)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Destination IP /Mask** Enter the destination IP address and netmask for this route.

**Gateway** Enter the IP address of the next hop router to which this route directs traffic

**Distance** The the relative preferability of this route. 1 is most preferred.

### To add a Transparent mode route

- 1 Go to **System > Network > Routing Table**.
- 2 Select Create New to add a new route.
- 3 Set the Destination IP and Mask to 0.0.0.0.  
For the default route, set the Destination IP and Mask to 0.0.0.0.



**Note:** Only one default route can be active at a time. If two default routes are added to the routing table, only the default route closest to the top of the routing table is active.

- 4 Set Gateway to the IP address of the next hop routing gateway.  
For an Internet connection, the next hop routing gateway routes traffic to the Internet.
- 5 Select OK to save the route.

## VLAN overview

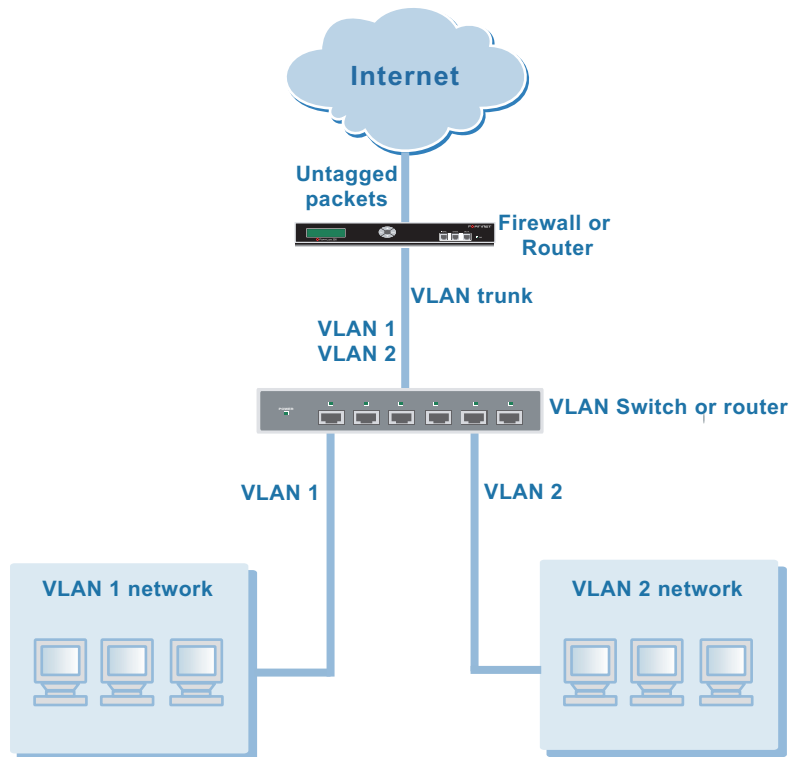
A VLAN is group of PCs, servers, and other network devices that communicate as if they were on the same LAN segment, even though they may not be. For example, the workstations and servers for an accounting department could be scattered throughout an office, connected to numerous network segments, but they can still belong to the same VLAN.

A VLAN segregates devices logically instead of physically. Each VLAN is treated as a broadcast domain. Devices in VLAN 1 can connect with other devices in VLAN 1, but cannot connect with devices in other VLANs. The communication among devices on a VLAN is independent of the physical network.

A VLAN segregates devices by adding 802.1Q VLAN tags to all of the packets sent and received by the devices in the VLAN. VLAN tags are 4-byte frame extensions that contain a VLAN identifier as well as other information.

VLANs allow highly flexible, efficient network segmentation, enabling users and resources to be grouped logically, regardless of physical locations.

Figure 14: Basic VLAN topology



### FortiGate units and VLANs

In a typical VLAN configuration, 802.1Q-compliant VLAN layer-2 switches or layer-3 routers or firewalls add VLAN tags to packets. Packets passing between devices in the same VLAN can be handled by layer 2 switches. Packets passing between devices in different VLANs must be handled by a layer 3 device such as router, firewall, or layer 3 switch.

Using VLANs, a single FortiGate unit can provide security services and control connections between multiple security domains. Traffic from each security domain is given a different VLAN ID. The FortiGate unit can recognize VLAN IDs and apply security policies to secure network and IPsec VPN traffic between security domains. The FortiGate unit can also apply authentication, protection profiles, and other firewall policy features for network and VPN traffic that is allowed to pass between security domains.

## VLANs in NAT/Route mode

Operating in NAT/Route mode, the FortiGate unit functions as a layer 3 device to control the flow of packets between VLANs. The FortiGate unit can also remove VLAN tags from incoming VLAN packets and forward untagged packets to other networks, such as the Internet.

In NAT/Route mode, the FortiGate units support VLANs for constructing VLAN trunks between an IEEE 802.1Q-compliant switch (or router) and the FortiGate unit. Normally the FortiGate unit internal interface connects to a VLAN trunk on an internal switch, and the external interface connects to an upstream Internet router untagged. The FortiGate unit can then apply different policies for traffic on each VLAN that connects to the internal interface.

In this configuration, you add VLAN subinterfaces to the FortiGate internal interface that have VLAN IDs that match the VLAN IDs of packets in the VLAN trunk. The FortiGate unit directs packets with VLAN IDs, to subinterfaces with matching VLAN IDs.

You can also define VLAN subinterfaces on all FortiGate interfaces. The FortiGate unit can add VLAN tags to packets leaving a VLAN subinterface or remove VLAN tags from incoming packets and add a different VLAN tags to outgoing packets.

## Rules for VLAN IDs

In NAT/Route mode, two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN IDs to different physical interfaces. There is no internal connection or link between two VLAN subinterfaces with same VLAN ID. Their relationship is the same as the relationship between any two FortiGate network interfaces.

## Rules for VLAN IP addresses

IP addresses of all FortiGate interfaces cannot overlap. That is, the IP addresses of all interfaces must be on different subnets. This rule applies to both physical interfaces and to VLAN subinterfaces.



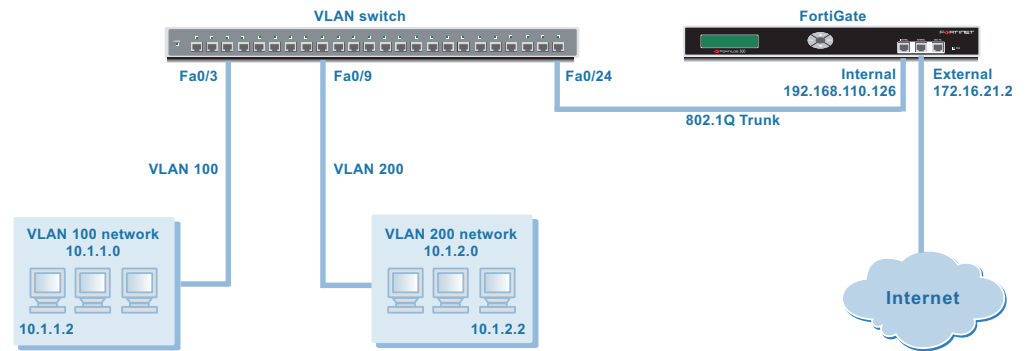
**Note:** If you are unable to change your existing configurations to prevent IP overlap, enter the CLI command `config system global and set ip-overlap enable` to allow IP address overlap. If you enter this command, multiple VLAN interfaces can have an IP address that is part of a subnet used by another interface. This command is recommended for advanced users only.

Figure 15 shows a simplified NAT/Route mode VLAN configuration. In this example, FortiGate internal interface connects to a VLAN switch using an 802.1Q trunk and is configured with two VLAN subinterfaces (VLAN 100 and VLAN 200). The external interface connects to the Internet. The external interface is not configured with VLAN subinterfaces.

When the VLAN switch receives packets from VLAN 100 and VLAN 200, it applies VLAN tags and forwards the packets to local ports and across the trunk to the FortiGate unit. The FortiGate unit is configured with policies that allow traffic to flow between the VLANs and from the VLANs to the external network.



Figure 15: FortiGate unit in Nat/Route mode



## Adding VLAN subinterfaces

The VLAN ID of each VLAN subinterface must match the VLAN ID added by the IEEE 802.1Q-compliant router. The VLAN ID can be any number between 1 and 4096. Each VLAN subinterface must also be configured with its own IP address and netmask.



**Note:** A VLAN must not have the same name as a virtual domain or zone.

You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.

### To add a VLAN subinterface in NAT/Route mode

- 1 Go to **System > Network > Interface**.
- 2 Select Create New to add a VLAN subinterface.
- 3 Enter a Name to identify the VLAN subinterface.
- 4 Select the physical interface that receives the VLAN packets intended for this VLAN subinterface.
- 5 Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface.
- 6 Select the virtual domain to which to add this VLAN subinterface.  
See [“System virtual domain” on page 131](#) for information about virtual domains.
- 7 Select the name of a zone if you want this VLAN subinterface to belong to a zone.  
You can only select a zone that has been added to the virtual domain selected in the previous step. See [“Zone” on page 58](#) for information about zones.
- 8 Configure the VLAN subinterface settings as you would for any FortiGate interface.  
See [“Interface settings” on page 48](#).
- 9 Select OK to save your changes.  
The FortiGate unit adds the new VLAN subinterface to the interface that you selected in step 4.

### To add firewall policies for VLAN subinterfaces

Once you have added VLAN subinterfaces you can add firewall policies for connections between VLAN subinterfaces or from a VLAN subinterface to a physical interface.

- 1 Go to **Firewall > Address**.
- 2 Select Create New to add firewall addresses that match the source and destination IP addresses of VLAN packets.  
See [“Address” on page 198](#).
- 3 Go to **Firewall > Policy**.
- 4 Add firewall policies as required.

## VLANs in Transparent mode

In Transparent mode, the FortiGate unit can apply firewall policies and services, such as authentication, protection profiles, and other firewall features, to traffic on an IEEE 802.1 VLAN trunk. You can insert the FortiGate unit operating in Transparent mode into the trunk without making changes to your network. In a typical configuration, the FortiGate internal interface accepts VLAN packets on a VLAN trunk from a VLAN switch or router connected to internal VLANs. The FortiGate external interface forwards tagged packets through the trunk to an external VLAN switch or router which could be connected to the Internet. The FortiGate unit can be configured to apply different policies for traffic on each VLAN in the trunk.

For VLAN traffic to be able to pass between the FortiGate Internal and external interface you would add a VLAN subinterface to the internal interface and another VLAN subinterface to the external interface. If these VLAN subinterfaces have the same VLAN IDs, the FortiGate unit applies firewall policies to the traffic on this VLAN. If these VLAN subinterfaces have different VLAN IDs, or if you add more than two VLAN subinterfaces, you can also use firewall policies to control connections between VLANs.

If the network uses IEEE 802.1 VLAN tags to segment your network traffic, you can configure a FortiGate unit operating in Transparent mode to provide security for network traffic passing between different VLANs. To support VLAN traffic in Transparent mode, you add virtual domains to the FortiGate unit configuration. A virtual domain consists of two or more VLAN subinterfaces or zones. In a virtual domain, a zone can contain one or more VLAN subinterfaces.

When the FortiGate unit receives a VLAN tagged packet at an interface, the packet is directed to the VLAN subinterface with matching VLAN ID. The VLAN subinterface removes the VLAN tag and assigns a destination interface to the packet based on its destination MAC address. The firewall policies for this source and destination VLAN subinterface pair are applied to the packet. If the packet is accepted by the firewall, the FortiGate unit forwards the packet to the destination VLAN subinterface. The destination VLAN ID is added to the packet by the FortiGate unit and the packet is sent to the VLAN trunk.

Figure 16: FortiGate unit with two virtual domains in Transparent mode

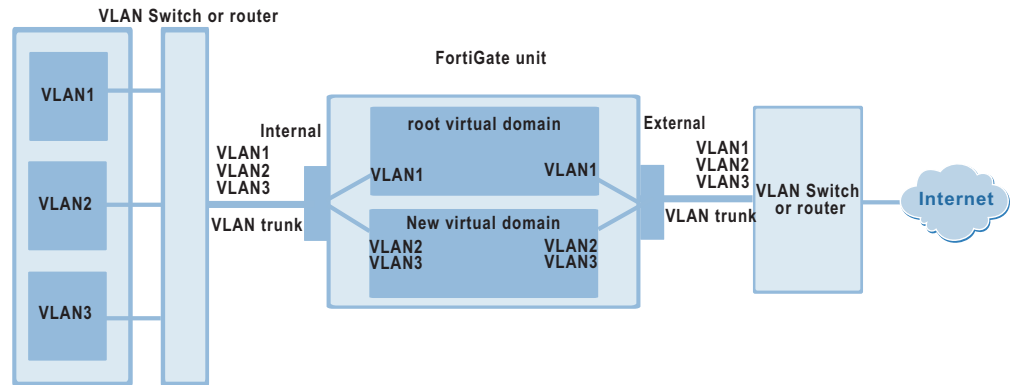
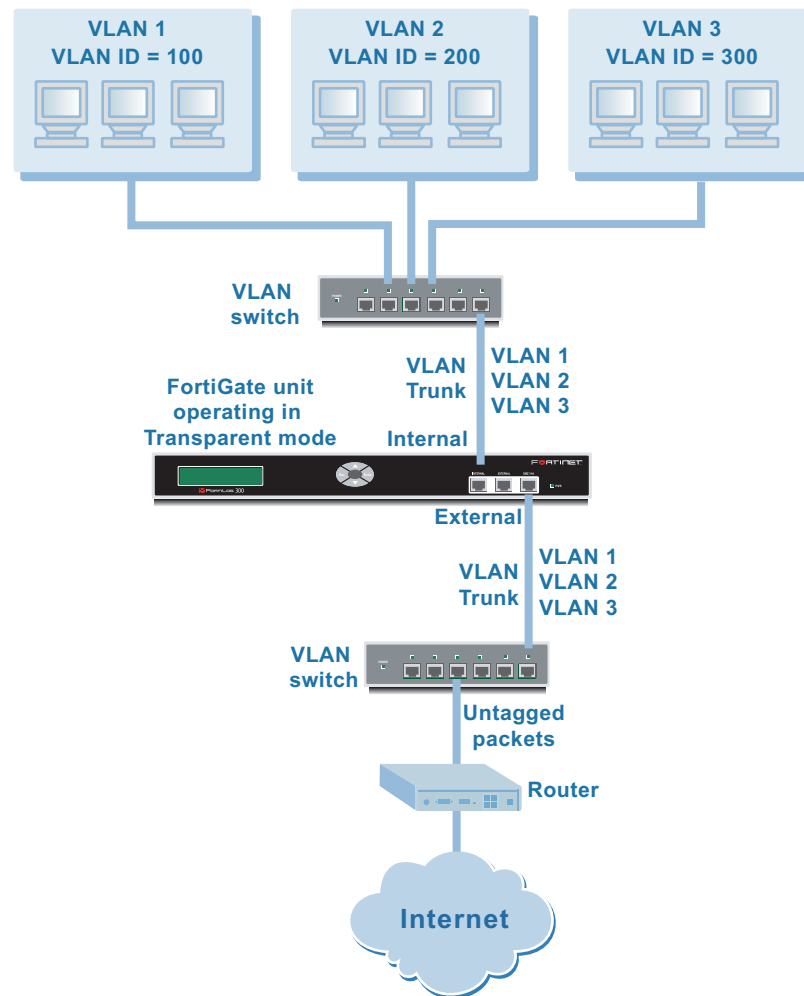


Figure 17 shows a FortiGate unit operating in Transparent mode and configured with three VLAN subinterfaces. In this configuration the FortiGate unit could be added to this network to provide virus scanning, web content filtering, and other services to each VLAN.

Figure 17: FortiGate unit in Transparent mode



## Rules for VLAN IDs

In Transparent mode two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN IDs to different physical interfaces. There is no internal connection or link between two VLAN subinterfaces with same VLAN ID. Their relationship is the same as the relationship between any two FortiGate network interfaces.

## Transparent mode virtual domains and VLANs

VLAN subinterfaces are added to and associated with virtual domains. By default the FortiGate configuration includes one virtual domain, named root, and you can add as many VLAN subinterfaces as you require to this virtual domain.

You can add more virtual domains if you want to separate groups of VLAN subinterfaces into virtual domains. For information on adding and configuring virtual domains, see [“System virtual domain” on page 131](#)

## Transparent mode VLAN list

In Transparent mode, go to **System > Network > Interface** to add VLAN subinterfaces.

**Figure 18: Sample Transparent mode VLAN list**

Name	Access	Status	
▼ <b>internal</b>	HTTPS,PING,SSH	➤ <b>Bring Down</b>	
int_vlan23		⊘ <b>Bring Up</b>	
▼ <b>external</b>	FING	➤ <b>Bring Down</b>	
ext_vlan23		⊘ <b>Bring Up</b>	

**Create New** Select Create New to add a VLAN subinterface to a FortiGate interface.

**Virtual Domain** Select a virtual domain to display the VLAN interfaces added to this virtual domain.

**Name** The name of the interface or VLAN subinterface.

**Access** The administrative access configuration for the interface. See [“To control administrative access to an interface” on page 57](#) for information about administrative access options.

**Status** The administrative status for the interface.  
 If the administrative status is a green arrow, the interface is up and can accept network traffic. If the administrative status is a red arrow, the interface is administratively down and cannot accept traffic. To change the administrative status, see [“To bring down an interface that is administratively up” on page 54](#) and [“To start up an interface that is administratively down” on page 54](#).

Delete icon. Select to delete a VLAN subinterface.

View/Edit icon. Select to view or edit an interface or VLAN subinterface.

## Transparent mode VLAN settings

VLAN settings displays the current configuration of a selected FortiGate interface or VLAN subinterface. Use VLAN settings to configure a new VLAN subinterface or to change the configuration of a FortiGate interface or VLAN subinterface.

**Figure 19: VLAN settings**

See [“Interface settings” on page 48](#) for descriptions of all VLAN settings.

### To add a VLAN subinterface in Transparent mode

The VLAN ID of each VLAN subinterface must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch. The VLAN ID can be any number between 1 and 4096. You add VLAN subinterfaces to the physical interface that receives VLAN-tagged packets.



**Note:** A VLAN must not have the same name as a virtual domain or zone.

- 1 Go to **System > Network > Interface**.
- 2 Select Create New to add a VLAN subinterface.
- 3 Enter a Name to identify the VLAN subinterface.
- 4 Select the physical interface that receives the VLAN packets intended for this VLAN subinterface.
- 5 Enter the VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface.
- 6 Select the virtual domain to which to add this VLAN subinterface.  
See [“System virtual domain” on page 131](#) for information about virtual domains.
- 7 Enable or disable using a Dynamic DNS service (DDNS). If the FortiGate unit uses a dynamic IP address, you can arrange with a DDNS service provider to use a domain name to provide redirection of traffic to your network whenever the IP address changes.
- 8 Configure the administrative access, MTU, and log settings as you would for any FortiGate interface.  
See [“Interface settings” on page 48](#) for more descriptions of these settings.
- 9 Select OK to save your changes.  
The FortiGate unit adds the new subinterface to the interface that you selected.
- 10 Select Bring up to start the VLAN subinterface.

### To add firewall policies for VLAN subinterfaces

Once you have added VLAN subinterfaces you can add firewall policies for connections between VLAN subinterfaces or from a VLAN subinterface to a physical interface.

- 1 Go to **Firewall > Address**.
- 2 Select Create New to add firewall addresses that match the source and destination IP addresses of VLAN packets.  
See [“Address” on page 198](#).
- 3 Go to **Firewall > Policy**.
- 4 Add firewall policies as required.

## FortiGate IPv6 support

You can assign both an IPv4 and an IPv6 address to any interface on a FortiGate unit. The interface functions as two interfaces, one for IPv4-addressed packets and another for IPv6-addressed packets.

FortiGate units support static routing, periodic router advertisements, and tunneling of IPv6-addressed traffic over an IPv4-addressed network. All of these features must be configured through the Command Line Interface (CLI). See the *FortiGate CLI Reference Guide* for information on the following commands:

**Table 2: IPv6 CLI commands**

Feature	CLI Command
Interface configuration, including periodic router advertisements	<code>config system interface</code> See the keywords beginning with "ip6". <code>config ip6-prefix-list</code>
Static routing	<code>config router static6</code>
IPv6 tunneling	<code>config system ipv6_tunnel</code>





## System DHCP

You can configure DHCP server or DHCP relay agent functionality on any FortiGate interface or VLAN subinterface.

A FortiGate interface can act as either a DHCP server or as a DHCP relay agent. An interface cannot provide both functions at the same time.



**Note:** To configure DHCP server or DHCP relay functionality on an interface, the FortiGate unit must be in NAT/Route mode and the interface must have a static IP address.

This section describes:

- [Service](#)
- [Server](#)
- [Exclude range](#)
- [IP/MAC binding](#)
- [Dynamic IP](#)

### Service

Go to **System > DHCP > Service** to configure the DHCP service provided by each FortiGate interface. You can configure each interface to be a DHCP relay or a DHCP server or you can turn off DHCP services.

**Figure 20: DHCP service list**

Interface	Service	
internal	None	
external	None	
dmz	None	

**Interface**

List of FortiGate interfaces.

**Service**

The DHCP service provided by the interface (none, DHCP Relay, or DHCP Server).

Edit/View icon. Select to view or modify the DHCP service configuration for an interface.

## DHCP service settings

Go to **System > DHCP > Service** and select an edit or view icon to view to modify the DHCP service configuration for an interface.

**Figure 21: View or edit DHCP service settings for an interface**

The screenshot shows a dialog box titled "Edit DHCP Service". At the top, it says "Interface: internal". Below that, there are three radio button options: "None", "DHCP Relay Agent", and "DHCP Server". The "DHCP Relay Agent" option is selected. Under "DHCP Relay Agent", there are two sub-options: "Regular" (selected) and "IPSEC". Below these, there is a text field for "DHCP Server IP" containing "0.0.0.0". At the bottom of the dialog, there are "OK" and "Cancel" buttons.

<b>Interface</b>	The name of the interface.
<b>None</b>	No DHCP services provided by the interface.
<b>DHCP Relay Agent</b>	Select to configure the interface to be a DHCP relay agent.
<b>Type</b>	Select the type of DHCP relay agent.
<b>Regular</b>	Configure the interface to be a DHCP relay agent for computers on the network connected to this interface. See <a href="#">"To configure an interface as a regular DHCP relay agent" on page 74.</a>
<b>IPSEC</b>	Configure the interface to be a DHCP relay agent only for remote VPN clients with an IPsec VPN connection to this interface that uses DHCP over IPsec.
<b>DHCP Server IP</b>	If you select DHCP Relay Agent, enter the IP address of the DHCP server used by the computers on the network connected to the interface.
<b>DHCP Server</b>	Select DHCP Server if you want the FortiGate unit to be the DHCP server. See <a href="#">"To configure an interface to be a DHCP server" on page 75.</a>

### To configure an interface as a regular DHCP relay agent

In a DHCP relay configuration, the FortiGate interface configured for DHCP relay forwards DHCP requests from DHCP clients through the FortiGate unit to a DHCP server. The FortiGate unit also returns responses from the DHCP server to the DHCP clients. The DHCP server must have a route to the FortiGate unit that is configured as the DHCP relay so that the packets sent by the DHCP server to the DHCP client arrive at the FortiGate performing DHCP relay.

- 1 Go to **System > DHCP > Service**.
- 2 Select Edit for the interface that you want to be a DHCP relay agent.
- 3 Select DHCP Relay Agent.
- 4 Set type to Regular.
- 5 Enter the DHCP Server IP address.
- 6 Select OK.

### To configure an interface to be a DHCP server

You can configure a DHCP server for any FortiGate interface. As a DHCP server, the interface dynamically assigns IP addresses to hosts on the network connected to the interface. You can also configure a DHCP server for more than one FortiGate interface.



- 1 Go to **System > DHCP > Service**.
- 2 Select Edit beside the interface to which you want to add a DHCP server.
- 3 Select DHCP Server.
- 4 Select OK.
- 5 Add a DHCP server configuration for this interface.  
See [“To configure a DHCP server for an interface” on page 76](#).

## Server

You can configure one or more DHCP servers for any FortiGate interface. As a DHCP server, the interface dynamically assigns IP addresses to hosts on a network connected to the interface.

You can add more than one DHCP server to a single interface to be able to provide DHCP services to multiple networks. For more information, see [“To configure multiple DHCP servers for an interface” on page 77](#).

**Figure 22: DHCP Server list**

Create New			
Name	Interface	Default Gateway	
DHCP_1	internal	220.200.10.0	 

<b>Create New</b>	Add a new DHCP server.
<b>Name</b>	Name of the DHCP server.
<b>Interface</b>	The interface for which the DHCP server is configured.
<b>Default Gateway</b>	The DHCP server configuration default gateway
<b>Delete</b>	Delete a DHCP server configuration.
<b>Edit/View icon</b>	View or modify a DHCP server configuration.

## DHCP server settings

Figure 23: Server options

<b>Name</b>	Enter a name for the DHCP server configuration.
<b>Interface</b>	Select the interface for which to configure the DHCP server.
<b>Domain</b>	Enter the domain that the DHCP server assigns to DHCP clients.
<b>Default Gateway</b>	Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
<b>IP Range</b>	Enter the starting IP and ending IP for the range of IP addresses that this DHCP server assigns to DHCP clients.
<b>Network Mask</b>	Enter the netmask that the DHCP server assigns to DHCP clients.
<b>Lease Time</b>	Select Unlimited for an unlimited lease time or enter the interval in days, hours, and minutes after which a DHCP client must ask the DHCP server for new settings. The lease time can range from 5 minutes to 100 days.
<b>DNS Server</b>	Enter the IP addresses of up to 3 DNS servers that the DHCP server assigns to DHCP clients.
<b>WINS Server</b>	Add the IP addresses of one or two WINS servers that the DHCP server assigns to DHCP clients.
<b>Option</b>	Up to three custom DHCP options that can be sent by the DHCP server. Code is the DHCP option code in the range 1 to 255. Option is an even number of hexadecimal characters and is not required for some option codes. For detailed information about DHCP options, see RFC 2132, DHCP Options and BOOTP Vendor Extensions.

### To configure a DHCP server for an interface

After configuring an interface to be a DHCP server (using the procedure [“To configure an interface to be a DHCP server” on page 75](#)), you must configure a DHCP server for the interface.

- 1 Go to **System > DHCP > Server**.
- 2 Select Create New.

- 3 Add a name for the DHCP server.
- 4 Select the interface
- 5 Configure the DHCP server.  
The IP range must match the subnet address of the network from which the DHCP request was received. Usually this would be the subnet connected to the interface for which you are added the DHCP server.
- 6 Select OK to save the DHCP server configuration.

### To configure multiple DHCP servers for an interface

If an interface is connected to a network that includes routers connected to different subnets, you can:

- 1 Configure computers on the subnets to get their IP configuration using DHCP.  
The IP range of each DHCP server must match the subnet addresses.
- 2 Configure the routers for DHCP relay.
- 3 Add multiple DHCP servers to the interface, one for each subnet.

When a computer on one of the connected subnets sends a DHCP request it is relayed to the FortiGate interface by the router, using DHCP relay. The FortiGate unit selects the DHCP server configuration with an IP range that matches the subnet address from which the DHCP request was received and uses this DHCP server to assign an IP configuration to the computer that made the DHCP request. The DHCP configuration packets are sent back to the router and the router relays them to the DHCP client.

## Exclude range

Add up to 16 exclude ranges of IP addresses that FortiGate DHCP servers cannot assign to DHCP clients. Exclude ranges apply to all FortiGate DHCP servers.

**Figure 24: Exclude range list**

#	Starting IP	Ending IP	
1	192.168.110.120	192.168.110.190	

<b>Create New</b>	Select Create New to add an exclude range.
<b>#</b>	The ID number of each exclude range. ID numbers are assigned sequentially by the web-based manager. When you add or edit exclude ranges from the CLI you must specify the ID number.
<b>Starting IP</b>	The starting IP of the exclude range.
<b>Ending IP</b>	The ending IP of the exclude range.
<b>Delete</b>	Delete an exclude range.
<b>Edit/View icon</b>	View or modify an exclude range.

## DHCP exclude range settings

The range cannot exceed 65536 IP addresses.

Figure 25: Exclude range settings

**Starting IP** Enter the starting IP of an exclude range.

**Ending IP** Enter the ending IP of an exclude range.

### To add an exclusion range

- 1 Go to **System > DHCP > Exclude Range**.
- 2 Select Create New.
- 3 Add the starting IP and ending IP.
- 4 Select OK to save the exclusion range.

## IP/MAC binding

If you have added DHCP servers, you can use DHCP IP/MAC binding to reserve an IP address for a particular device on the network according to the MAC address of the device. When you add the MAC address and an IP address to the IP/MAC binding list, the DHCP server always assigns this IP address to the MAC address. IP/MAC binding pairs apply to all FortiGate DHCP servers.

Figure 26: IP/MAC binding list

Name	IP Address	MAC Address	
Server_1	192.168.110.50	b3:45:ff:21:da:00	
Server_2	192.166.110.60	63:bb:d8:a1:f3:32	

**Create New** Select Create New to add a DHCP IP/MAC binding pair.

**Name** The name for the IP and MAC address pair.

**IP Address** The IP address for the IP and MAC address pair. The IP address must be within the configured IP range.

**MAC Address** The MAC address of the device.

Delete icon. Delete an IP/MAC binding pair.

Edit/View icon. View or modify an IP/MAC binding pair.

## DHCP IP/MAC binding settings

Figure 27: IP/MAC binding options

New IP/MAC Binding	
Name	IPMAC_3
IP Address	10.10.10.45
MAC Address	00:10:F3:04:7A:4A
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- Name** Enter a name for the IP/MAC address pair.
- IP Address** Enter the IP address for the IP and MAC address pair. The IP address must be within the configured IP range.
- MAC Address** Enter the MAC address of the device.

### To add a DHCP IP/MAC binding pair

- 1 Go to **System > DHCP > IP/MAC Binding**.
- 2 Select Create New.
- 3 Add a name for the IP/MAC pair.
- 4 Add the IP address and MAC address.
- 5 Select OK to save the IP/MAC pair.

## Dynamic IP

You can view the list of IP addresses that the DHCP server has assigned, their corresponding MAC addresses, and the expiry time and date for these addresses.

- Interface** Select to display its dynamic IP list.
- IP** The IP addresses that the DHCP server has assigned.
- MAC** The corresponding MAC addresses for the dynamic IP addresses.
- Expire** The expiry time and date for the dynamic IP addresses and their corresponding MAC addresses.

### To view the dynamic IP list

- 1 Go to **System > DHCP > Dynamic IP**.
- 2 Select the interface for which you want to view the list.





## System config

Use the System Config page to make any of the following changes to the FortiGate system configuration:

- [System time](#)
- [Options](#)
- [HA](#)
- [SNMP](#)
- [Replacement messages](#)
- [FortiManager](#)

### System time

Go to **System > Config > Time** to set the FortiGate system time.

For effective scheduling and logging, the FortiGate system time must be accurate. You can either manually set the FortiGate system time or you can configure the FortiGate unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

**Figure 28: System time**

The screenshot shows the 'Time Settings' configuration page. At the top, the 'System Time' is displayed as 'Sun Mar 21 15:31:05 2004' with a 'Refresh' button. Below this, the 'Time Zone' is set to '(GMT-8:00)Pacific Time(US&Canada)'. There is a checkbox for 'Automatically adjust clock for daylight saving changes' which is currently unchecked. Two radio buttons are present: 'Set Time' (selected) and 'Synchronize with NTP Server'. Under 'Set Time', there are dropdown menus for Hour (15), Minute (31), Second (5), Month (Mar), Day (21), and Year (2004). Under 'Synchronize with NTP Server', there is a text input for 'Server' (132.246.168.148) and a dropdown for 'Syn Interval' (60 mins). An 'Apply' button is at the bottom.

<b>System Time</b>	The current FortiGate system date and time.
<b>Refresh</b>	Select Refresh to update the display of the current FortiGate system date and time.
<b>Time Zone</b>	Select the current FortiGate system time zone.

<b>Automatically adjust clock for daylight saving changes</b>	Select the Automatically adjust clock for daylight saving changes check box if you want the FortiGate system clock to be adjusted automatically when your time zone changes to daylight saving time and back to standard time.
<b>Set Time</b>	Select Set Time to set the FortiGate system date and time to the correct date and time.
<b>Synchronize with NTP Server</b>	Select Synchronize with NTP Server to configure the FortiGate unit to use NTP to automatically set the system date and time. For more information about NTP and to find the IP address of an NTP server that you can use, see <a href="http://www.ntp.org">http://www.ntp.org</a> .
<b>Server</b>	Enter the IP address or domain name of the NTP server that the FortiGate unit can use to set its time and date.
<b>Syn Interval</b>	Specify how often the FortiGate unit should synchronize its time with the NTP server. A typical Syn Interval would be 1440 minutes for the FortiGate unit to synchronize its time once a day.

#### To manually set the FortiGate date and time

- 1 Go to **System > Config > Time**.
- 2 Select Refresh to display the current FortiGate system date and time.
- 3 Select your Time Zone from the list.
- 4 Optionally, select Automatically adjust clock for daylight saving changes check box.
- 5 Select Set Time and set the FortiGate system date and time.
- 6 Set the hour, minute, second, month, day, and year as required.
- 7 Select Apply.

#### To use NTP to set the FortiGate date and time

- 1 Go to **System > Config > Time**.
- 2 Select Synchronize with NTP Server to configure the FortiGate unit to use NTP to automatically set the system time and date.
- 3 Enter the IP address or domain name of the NTP server that the FortiGate unit can use to set its time and date.
- 4 Specify how often the FortiGate unit should synchronize its time with the NTP server.
- 5 Select Apply.

## Options

Go to **System > Config > Options** to set the following options:

- Timeout settings including the idle timeout and authentication timeout
- The language displayed by the web-based manager
- Dead gateway detection interval and failover detection

Figure 29: System config options

Configuration Options		
<b>Timeout Settings</b>		
Idle Timeout	<input type="text" value="50"/>	(1-480 mins)
Auth Timeout	<input type="text" value="15"/>	(1-480 mins)
<b>Web Administration</b>		
Language	<input type="text" value="English"/>	
<b>Dead Gateway Detection</b>		
Detection Interval	<input type="text" value="5"/>	(seconds)
Fail-over Detection	<input type="text" value="5"/>	(lost consecutive pings)
<input type="button" value="Apply"/>		

- Idle Timeout** Set the idle time out to control the amount of inactive time before the administrator must log in again. The maximum `admintimeout` is 480 minutes (8 hours). To improve security keep the idle timeout at the default value of 5 minutes.
- Auth Timeout** Set the firewall user authentication timeout to control how long an authenticated connection can be idle before the user must authenticate again. The maximum `authtimeout` is 480 minutes (8 hours). The default Auth Timeout is 15 minutes.  
For more information, see [“Setting authentication timeout” on page 234](#).
- Language** Select a language for the web-based manager to use. Choose from English, Simplified Chinese, Japanese, Korean, or French.
- Detection Interval** Set the dead gateway detection failover interval. Enter a number in seconds to specify how often the FortiGate unit pings the target.
- Fail-over Detection** Set the ping server dead gateway detection failover number. Enter the number of times that ping fails before the FortiGate unit assumes that the gateway is no longer functioning.

#### To set the system idle timeout

- 1 Go to **System > Config > Options**.
- 2 For Idle Timeout, type a number in minutes.
- 3 Select Apply.

#### To set the Auth timeout

- 1 Go to **System > Config > Options**.
- 2 For Auth Timeout, type a number in minutes.
- 3 Select Apply.

#### To select a language for the web-based manager

- 1 Go to **System > Config > Options**.
- 2 From the Languages list, select a language for the web-based manager to use.
- 3 Select Apply.



**Note:** You should select the language that the management computer operating system uses.

### To modify the dead gateway detection settings

Modify dead gateway detection to control how the FortiGate unit confirms connectivity with a ping server added to an interface configuration. For information about adding a ping server to an interface, see [“To add a ping server to an interface” on page 56](#).

- 1 Go to **System > Config > Options**.
- 2 For Detection Interval, type a number in seconds to specify how often the FortiGate unit tests the connection to the ping target.
- 3 For Fail-over Detection, type a number of times that the connection test fails before the FortiGate unit assumes that the gateway is no longer functioning.
- 4 Select Apply.

## HA

Fortinet achieves high availability (HA) using redundant hardware and the FortiGate Clustering Protocol (FGCP). Each FortiGate unit in an HA cluster enforces the same overall security policy and shares the same configuration settings. You can add up to 32 FortiGate units to an HA cluster. Each FortiGate unit in an HA cluster must be the same model and must be running the same FortiOS firmware image.

The FortiGate units in the cluster use cluster ethernet interfaces to communicate cluster session information, synchronize the cluster configuration, synchronize the cluster routing table, and report individual cluster member status. The units in the cluster are constantly communicating HA status information to make sure that the cluster is operating properly. This communication is called the HA heartbeat.

FortiGate HA supports link failover, device failover, and HA heartbeat failover.

**Link failover** If one of the links to a FortiGate unit in an HA cluster fails, all functions, all established firewall connections, and all IPSec VPN sessions<sup>a</sup> are maintained by the other FortiGate units in the HA cluster. For information about link failover, see [“Monitor priorities” on page 90](#).

**Device failover** If one of the FortiGate units in an HA cluster fails, all functions, all established firewall connections, and all IPSec VPN sessions are maintained by the other FortiGate units in the HA cluster.

**HA heartbeat failover** You can configure multiple interfaces to be HA heartbeat devices. If an interface functioning as an HA heartbeat device fails, the HA heartbeat is transferred to another interface also configured as an HA heartbeat device.

a. HA does not provide session failover for PPPoE, DHCP, PPTP, and L2TP services.

FortiGate units can be configured to operate in active-passive (A-P) or active-active (A-A) HA mode. Active-active and active-passive clusters can run in either NAT/Route or Transparent mode.

An active-passive (A-P) HA cluster, also referred to as hot standby HA, consists of a primary FortiGate unit that processes traffic, and one or more subordinate FortiGate units. The subordinate FortiGate units are connected to the network and to the primary FortiGate unit but do not process traffic.

Active-active (A-A) HA load balances network traffic all the FortiGate units in the cluster. An active-active HA cluster consists of a primary FortiGate unit that processes traffic and one or more subordinate units that also process traffic. The primary FortiGate unit uses a load balancing algorithm to distribute virus scanning to all the FortiGate units in the HA cluster.

By default the FortiGate unit load balances virus scanning among all of the FortiGate units in the cluster. Using the CLI, you can configure the FortiGate unit to load balance all network traffic among the FortiGate units in the cluster. See the *FortiGate CLI Reference Guide* for more information.

For more information about FortiGate HA and the FGCP, see the *FortiGate High Availability Guide*.

## HA configuration

Go to **System > Config > HA** and use the options described below to configure HA.

**Figure 30: HA configuration**

Interface	Heartbeat Device	Monitor
internal	<input type="checkbox"/> Enable priority: <input type="text"/>	<input checked="" type="checkbox"/> Enable priority: <input type="text"/>
external	<input checked="" type="checkbox"/> Enable priority: <input type="text"/>	<input checked="" type="checkbox"/> Enable priority: <input type="text"/>
dmz	<input checked="" type="checkbox"/> Enable priority: <input type="text"/>	<input type="checkbox"/> Enable priority: <input type="text"/>

### Standalone Mode

Standalone mode is the default operation mode. If Standalone mode is selected the FortiGate unit is not operating in HA mode.

Select Standalone Mode if you want to stop a cluster unit from operating in HA mode.

### High Availability

Select High Availability to operate the FortiGate unit in HA mode. After selecting High Availability, complete the remainder of the HA configuration.

## Cluster Members

When the cluster is operating, you can select Cluster Members to view the status of all FortiGate units in the cluster. Status information includes the cluster ID, status, up time, weight, and monitor information. For more information, see [“To view the status of each cluster member” on page 94](#).

## Mode

All members of the HA cluster must be set to the same HA mode.

**Active-Active** Load balancing and failover HA. Each cluster unit actively processes connections and monitors the status of the other FortiGate units in the cluster. The primary FortiGate unit in the cluster controls load balancing among all of the cluster units.

**Active-Passive** Failover HA. The primary FortiGate unit in the cluster processes all connections. All other FortiGate units in the cluster passively monitor the cluster status and remain synchronized with the primary FortiGate unit.

## Group ID

The group ID range is from 0 to 63. All members of the HA cluster must have the same group ID.

When the FortiGate units in the cluster are switched to HA mode, all of the interfaces of all of the units in the cluster acquire the same virtual MAC address. This virtual MAC address is set according to the group ID. [Table 3](#) lists the virtual MAC address set for each group ID.

**Table 3: HA group ID and MAC address**

Group ID	MAC Address
0	00-09-0f-06-ff-00
1	00-09-0f-06-ff-01
2	00-09-0f-06-ff-02
3	00-09-0f-06-ff-03
...	...
63	00-09-0f-06-ff-3f

If you have more than one HA cluster on the same network, each cluster should have a different group ID. If two clusters on the same network have the same group ID, the duplicate MAC addresses cause addressing conflicts on the network.

## Unit Priority

Optionally set the unit priority of the cluster unit. Each cluster unit can have a different unit priority (the unit priority is not synchronized among cluster members). During HA negotiation, the unit with the highest unit priority becomes the primary cluster unit. The unit priority range is 0 to 255. The default unit priority is 128.

You can use the unit priority to control the order in which cluster units become the primary cluster unit when a cluster unit fails. For example, if you have three FortiGate-3600s in a cluster you can set the unit priorities as shown in [Table 4](#). Cluster unit A will always be the primary cluster unit because it has the highest priority. If cluster unit A fails, cluster unit B becomes the primary cluster unit because cluster unit B has a higher unit priority than cluster unit C.

**Table 4: Example unit priorities for a cluster of three cluster units**

Cluster unit	Unit priority
A	200
B	100
C	50

The unit priority is not synchronized to all cluster units. Each cluster unit can have a different unit priority.

In a functioning cluster, if you change the unit priority of the current primary cluster unit to a lower priority, when the cluster renegotiates a different cluster unit becomes the primary cluster unit.

### Override Master

Configure a cluster unit to always override the current primary cluster unit and become the primary cluster unit. Enable override master for the cluster unit that you have given the highest unit priority. Enabling Override Master means that this cluster unit always becomes the primary cluster unit.

In a typical FortiGate cluster configuration, the primary unit is selected automatically. In some situations, you might want to control which unit becomes the primary unit. You can configure a FortiGate unit as the permanent primary unit by setting a high unit priority and by selecting override master. With this configuration, the same cluster unit always becomes the primary cluster unit.

If override master is enabled and the primary cluster unit fails another cluster unit becomes the primary unit. When the cluster unit with override master enabled rejoins the cluster it overrides the current primary unit and becomes the new primary unit. When this override occurs, all communication sessions through the cluster are lost and must be re-established.

Override master is not synchronized to all cluster units.

In a functioning cluster, if you select override master for a cluster unit the cluster negotiates and may select a new primary cluster unit.

### Password

Enter a password for the HA cluster. The password must be the same for all FortiGate units in the HA cluster. The maximum password length is 15 characters.

If you have more than one FortiGate HA cluster on the same network, each cluster should have a different password.

## Schedule

If you are configuring an active-active cluster, select a load balancing schedule.

<b>None</b>	No load balancing. Select None when the cluster interfaces are connected to load balancing switches.
<b>Hub</b>	Load balancing if the cluster interfaces are connected to a hub. Traffic is distributed to cluster units based on the Source IP and Destination IP of the packet.
<b>Least-Connection</b>	Least connection load balancing. If the cluster units are connected using switches, select Least Connection to distribute network traffic to the cluster unit currently processing the fewest connections.
<b>Round-Robin</b>	Round robin load balancing. If the cluster units are connected using switches, select Round-Robin to distribute network traffic to the next available cluster unit.
<b>Weighted Round-Robin</b>	Weighted round robin load balancing. Similar to round robin, but weighted values are assigned to each of the units in a cluster based on their capacity and on how many connections they are currently processing. For example, the primary unit should have a lower weighted value because it handles scheduling and forwards traffic. Weighted round robin distributes traffic more evenly because units that are not processing traffic will be more likely to receive new connections than units that are very busy.
<b>Random</b>	Random load balancing. If the cluster units are connected using switches, select Random to randomly distribute traffic to cluster units.
<b>IP</b>	Load balancing according to IP address. If the cluster units are connected using switches, select IP to distribute traffic to units in a cluster based on the Source IP and Destination IP of the packet.
<b>IP Port</b>	Load balancing according to IP address and port. If the cluster units are connected using switches, select IP Port to distribute traffic to units in a cluster based on the source IP, source port, destination IP, and destination port of the packet.

## Priorities of Heartbeat Device

Enable or disable HA heartbeat communication and set the heartbeat priority for each interface in the cluster.

By default HA heartbeat communication is set for two interfaces. You can disable HA heartbeat communication for either of these interfaces or enable HA heartbeat for other interfaces. In most cases you can maintain the default heartbeat device configuration as long as you can connect the heartbeat device interfaces together.

To enable HA heartbeat communication for an interface, enter a priority for the interface. To disable HA heartbeat communication for an interface, delete the priority for the interface.

The HA heartbeat priority range is 0 to 512. The interface with the highest priority handles all HA heartbeat traffic. If this interface fails or becomes disconnected, the interface with the next highest priority handles all HA heartbeat traffic.

The cluster units use the ethernet interfaces configured with HA heartbeat priorities for HA heartbeat communication. The HA heartbeat communicates cluster session information, synchronizes the cluster configuration, synchronizes the cluster routing table, and reports individual cluster member status. The HA heartbeat constantly communicates HA status information to make sure that the cluster is operating properly.



You can enable heartbeat communications for physical interfaces, but not for VLAN subinterfaces.

Enabling the HA heartbeat for more interfaces increases reliability. If an interface fails, the HA heartbeat can be diverted to another interface.

HA heartbeat traffic can use a considerable amount of network bandwidth. If possible, enable HA heartbeat traffic on interfaces only used for HA heartbeat traffic or on interfaces connected to less busy networks.

**Table 5: Default heartbeat device configuration**

FortiGate model	Default heartbeat device	Default priority
FortiGate-200	External	50
	DMZ	100

Change the heartbeat device priorities as required to control the interface that is used for heartbeat traffic and the interface to which heartbeat traffic reverts if the interface with the highest heartbeat priority fails or is disconnected.

Setting the heartbeat priority for more interfaces increases the reliability of the cluster. To optimize bandwidth use, you can route most heartbeat traffic to interfaces that handle less network traffic. You can also create a failover path by setting heartbeat priorities so that you can control the order in which interfaces are used for heartbeat traffic.

The heartbeat priority must be set for at least one cluster interface. If heartbeat communication is interrupted the cluster stops processing traffic.

## Heartbeat device IP addresses

You do not need to assign IP addresses to the heartbeat device interfaces for them to be able to process heartbeat packets. In HA mode the cluster assigns virtual IP addresses to the heartbeat device interfaces. The primary cluster unit heartbeat device interface is assigned the IP address 10.0.0.1 and the subordinate unit is assigned the IP address 10.0.0.2. A third cluster unit would be assigned the IP address 10.0.0.3 and so on.

For best results, isolate each heartbeat device on its own network. Heartbeat packets contain sensitive information about the cluster configuration. Also, heartbeat packets may use a considerable amount of network bandwidth and it is preferable to isolate this traffic from your user networks. The extra bandwidth used by heartbeat packets could also reduce the capacity of the interface to process network traffic.

For most FortiGate models if you do not change the heartbeat device configuration, you would isolate the HA interfaces of all of the cluster units by connecting them all to the same switch. If the cluster consists of two FortiGate units you can connect the heartbeat device interfaces directly using a crossover cable.

HA heartbeat and data traffic are supported on the same FortiGate interface. In NAT/Route mode, if you decide to use the heartbeat device interfaces for processing network traffic or for a management connection, you can assign the interface any IP address. This IP address does not affect the heartbeat traffic. In Transparent mode, you can connect the interface to your network.

## Monitor priorities

Enable or disable monitoring a FortiGate interface to verify that the interface is functioning properly and connected to its network. If a monitored interface fails or is disconnected from its network the interface leaves the cluster. The cluster reroutes the traffic being processed by that interface to the same interface of another cluster unit in the cluster that still has a connection to the network. This other cluster unit becomes the new primary cluster unit.

If you can re-establish traffic flow through the interface (for example, if you re-connect a disconnected network cable) the interface rejoins the cluster. If Override Master is enabled for this FortiGate unit (see [“Override Master” on page 87](#)), this FortiGate unit becomes the primary unit in the cluster again.



**Note:** Only monitor interfaces that are connected to networks.



**Note:** You can monitor physical interfaces, but not VLAN subinterfaces.

Increase the priority of interfaces connected to higher priority networks or networks with more traffic. The monitor priority range is 0 to 512.

If a high priority interface on the primary cluster unit fails, one of the other units in the cluster becomes the new primary unit to provide better service to the high priority network.

If a low priority interface fails on one cluster unit and a high priority interface fails on another cluster unit, a unit in the cluster with a working connection to the high priority interface would, if it becomes necessary to negotiate a new primary unit, be selected instead of a unit with a working connection to the low priority interface.

## Configuring an HA cluster

Use the following procedures to create an HA cluster consisting of two or more FortiGate units. These procedures describe how to configure each of the FortiGate units for HA operation and then how to connect the FortiGate units to form a cluster. Once the cluster is connected you can configure it in the same way as you would configure a standalone FortiGate unit.

### To configure a FortiGate unit for HA operation

Each FortiGate unit in the cluster must have the same HA configuration. Use the following procedure to configure each FortiGate unit for HA operation.



**Note:** The following procedure does not include steps for configuring interface heartbeat devices and interface monitoring. Both of these HA settings should be configured after the cluster is up and running.

- 1 Power on the FortiGate unit to be configured.
- 2 Connect to the web-based manager.

- 3 Give the FortiGate unit a unique host name.  
See [“To change FortiGate host name” on page 30](#). Use host names to identify individual cluster units.
- 4 Go to **System > Config > HA**.
- 5 Select HA.
- 6 Select the HA mode.
- 7 Select a Group ID for the cluster.  
The Group ID must be the same for all FortiGate units in the HA cluster.
- 8 Optionally change the Unit Priority.  
See [“Unit Priority” on page 86](#).
- 9 If required, select Override master.  
See [“Override Master” on page 87](#).
- 10 Enter and confirm a password for the HA cluster.
- 11 If you are configuring Active-Active HA, select a schedule.  
See [“Schedule” on page 88](#).
- 12 Select Apply.  
The FortiGate unit negotiates to establish an HA cluster. When you select apply you may temporarily lose connectivity with the FortiGate unit as the HA cluster negotiates.
- 13 If you are configuring a NAT/Route mode cluster, power off the FortiGate unit and then repeat this procedure for all the FortiGate units in the cluster. Once all of the units are configured, continue with [“To connect a FortiGate HA cluster” on page 91](#).
- 14 If you are configuring a Transparent mode cluster, reconnect to the web-based manager.  
You may have to wait a few minutes before you can reconnect.
- 15 Go to **System > Status**.
- 16 Select Change to Transparent Mode and select OK to switch the FortiGate unit to Transparent mode.
- 17 Power off the FortiGate unit.
- 18 Repeat this procedure for all of the FortiGate units in the cluster then continue with [“To connect a FortiGate HA cluster” on page 91](#).

#### **To connect a FortiGate HA cluster**

Use the following procedure to connect a cluster operating in NAT/Route mode or Transparent mode. Connect the FortiGate units in the cluster to each other and to your network. You must connect all matching interfaces in the cluster to the same hub or switch. Then you must connect these interfaces to their networks using the same hub or switch.

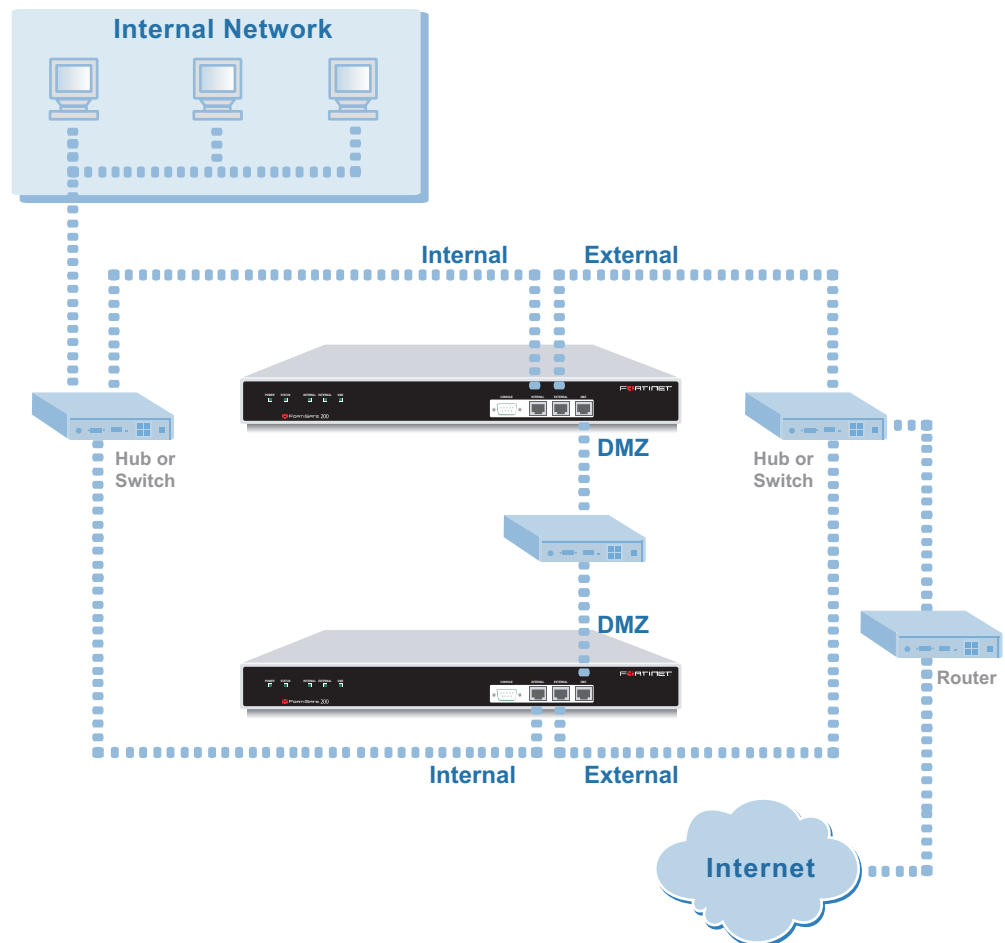
Fortinet recommends using switches for all cluster connections for the best performance.

The FortiGate units in the cluster use cluster ethernet interfaces to communicate cluster session information, synchronize the cluster configuration, and report individual cluster member status. The units in the cluster are constantly communicating HA status information to make sure that the cluster is operating properly. This cluster communication is also called the cluster heartbeat.

Inserting an HA cluster into your network temporarily interrupts communications on the network because new physical connections are being made to route traffic through the cluster. Also, starting the cluster interrupts network traffic until the individual FortiGate units in the cluster are functioning and the cluster completes negotiation. Cluster negotiation normally takes just a few seconds. During system startup and negotiation all network traffic is dropped.

- 1 Connect the cluster units.
  - Connect the internal interfaces of each FortiGate unit to a switch or hub connected to your internal network.
  - Connect the external interfaces of each FortiGate unit to a switch or hub connected to your external network.
  - Connect the DMZ interfaces of the FortiGate units to another switch or hub.

**Figure 31: HA network configuration**



- 2 Power on all the FortiGate units in the cluster.  
As the units start, they negotiate to choose the primary cluster unit and the subordinate units. This negotiation occurs with no user intervention and normally just takes a few seconds.

You can now configure the cluster as if it is a single FortiGate unit.

#### To add a new unit to a functioning cluster

- 1 Configure the new FortiGate unit for HA operation with the same HA configuration as the other units in the cluster.
- 2 If the cluster is running in Transparent mode, change the operating mode of the new FortiGate unit to Transparent mode.
- 3 Connect the new FortiGate unit to the cluster.
- 4 Power on the new FortiGate unit.  
When the unit starts it negotiates to join the cluster. After it joins the cluster, the cluster synchronizes the new unit configuration with the configuration of the primary unit.

#### To configure weighted-round-robin weights

By default, in active-active HA mode the weighted round-robin schedule assigns the same weight to each FortiGate unit in the cluster. If you configure a cluster to use the weighted round-robin schedule, from the CLI you can use `config system ha weight` to configure a weight value for each cluster unit. The weight value sets the maximum number of connections that are sent to a cluster unit before a connection can be sent to the next cluster unit. You can set weight values to control the number of connections processed by each cluster unit. For example, you might want to reduce the number of connections processed by the primary cluster unit by increasing the weight assigned to the subordinate cluster units.

Weight values are entered as two values; the priority order of the unit in the cluster (in the range 0 to 31) followed by its weight (also in the range 0 to 31). For example, if you have a cluster of three FortiGate units, you can enter the following command to configure the weight values for each unit:

```
config system ha
  set ha weight 0 1 1 3 2 3
end
```

This command has the following results:

- The first connection is processed by the primary unit (priority 0, weight 1)
- The next three connections are processed by the first subordinate unit (priority 1, weight 3)
- The next three connections are processed by the second subordinate unit (priority 2, weight 3)

The subordinate units process more connections than the primary unit, and both subordinate units, on average, process the same number of connections.

## Managing an HA cluster

The configurations of all of the FortiGate units in the cluster are synchronized so that the FortiGate units can function as a cluster. Because of this synchronization, you manage the HA cluster instead of managing the individual FortiGate units in the cluster. You manage the cluster by connecting to the web-based manager using any cluster interface configured for HTTPS administrative access. You can also manage the cluster by connecting to the CLI using any cluster interface configured for SSH administrative access.

You can also use SNMP to manage the cluster by configuring a cluster interface for SNMP administrative access. Using an SNMP manager you can get cluster configuration information and receive traps. For a list of HA MIB fields, see [“HA MIB fields” on page 104](#) and [“FortiGate HA traps” on page 103](#).

You can change the cluster configuration by connecting to the cluster and changing the configuration of the primary FortiGate unit. The cluster automatically synchronizes all configuration changes to the subordinate units in the cluster as the changes are made.

The only configuration change that is not synchronized is the FortiGate host name. You can give each cluster unit a unique host name to help to identify cluster members.

You can use the web-based manager to monitor the status and logs of individual cluster members. See [“To view the status of each cluster member” on page 94](#) and [“To view and manage logs for individual cluster units” on page 95](#).

You can manage individual cluster units by using SSH to connect to the CLI of the cluster. From the CLI you can use the `execute ha manage` command to connect to the CLI of each unit in the cluster. You can also manage individual cluster units by using a null-modem cable to connect to the primary cluster unit. From there you can also use the `execute ha manage` command to connect to the CLI of each unit in the cluster. See [“To manage individual cluster units” on page 96](#) for more information.

### To view the status of each cluster member

- 1 Connect to the cluster and log into the web-based manager.
- 2 Go to **System > Config > HA**.
- 3 Select Cluster Members.

A list of cluster members appears. The list includes the cluster ID of each cluster member as well as status information for each cluster member.

Figure 32: Example cluster members list (active-active cluster)

Refresh every		10 seconds		Go		<a href="#">Back to HA configuration page &gt;&gt;</a>	
Cluster ID	Status	Up Time	Monitor				
FGT5002801021077	✓	1 days 23 hours 7 minutes 46 seconds	CPU Usage 	Active Sessions	Total Packets	Virus Detected	
			Memory Usage 	Network Utilization	Total Bytes	Intrusion Detected	
FGTE002803033050	✓	1 days 5 hours 51 minutes 56 seconds	CPU Usage 	Active Sessions	Total Packets	Virus Detected	
			Memory Usage 	Network Utilization	Total Bytes	Intrusion Detected	

<b>Refresh every</b>	Select to control how often the web-based manager updates the system status display.
<b>Go</b>	Select to set the selected refresh interval.
<b>Back to HA configuration page</b>	Close the cluster members list and return to the HA configuration page.
<b>Cluster ID</b>	Use the cluster ID to identify each FortiGate unit in the cluster. The cluster ID matches the FortiGate unit serial number.
<b>Status</b>	Indicates the status of each cluster unit. A green check mark indicates that the cluster unit is operating normally. A red X indicates that the cluster unit cannot communicate with the primary unit.
<b>Up Time</b>	The time in days, hours, minutes, and seconds since the cluster unit was last started.
<b>Monitor</b>	Displays system status information for each cluster unit.
<b>CPU Usage</b>	The current CPU status of each cluster unit. The web-based manager displays CPU usage for core processes only. CPU usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
<b>Memory Usage</b>	The current memory status of each cluster unit. The web-based manager displays memory usage for core processes only. Memory usage for management processes (for example, for HTTPS connections to the web-based manager) is excluded.
<b>Active Sessions</b>	The number of communications sessions being processed by the each cluster unit.
<b>Total Packets</b>	The number of packets that have been processed by the cluster unit since it last started up.
<b>Virus Detected</b>	The number of viruses detected by the cluster unit.
<b>Network Utilization</b>	The total network bandwidth being used by all of the cluster unit interfaces.
<b>Total Bytes</b>	The number of bytes that have been processed by the cluster unit since it last started up.
<b>Intrusion Detected</b>	The number of intrusions or attacks detected by the cluster unit.

### To view and manage logs for individual cluster units

- 1 Connect to the cluster and log into the web-based manager.

**2 Go to **Log&Report > Log Access.****

The Traffic log, Event log, Attack log, Antivirus log, Web Filter log, and Email Filter log for the primary unit are displayed.

The HA Cluster pull-down list displays the serial number of the FortiGate unit for which logs are displayed.

**3 Select the serial number of one of the FortiGate units in the cluster to display the logs for that FortiGate unit.**

You can view, search and manage logs saved to memory or logs saved to the hard disk, depending on the configuration of the cluster unit.

**To monitor cluster units for failover**

If the primary unit in the cluster fails, the units in the cluster renegotiate to select a new primary unit. Failure of the primary unit results in the following:

- If SNMP is enabled, the new primary FortiGate unit sends the trap message “HA switch”. This trap indicates that the primary unit in an HA cluster has failed and has been replaced with a new primary unit.
- The cluster contains fewer FortiGate units. The failed primary unit no longer appears on the Cluster Members list.
- The host name and serial number of the primary cluster unit changes.
- The new primary unit logs the following messages to the event log:

```
HA slave became master
Detected HA member dead
```

If a subordinate unit fails, the cluster continues to function normally. Failure of a subordinate unit results in the following:

- The cluster contains fewer FortiGate units. The failed unit no longer appears on the Cluster Members list.
- The master unit logs the following message to the event log:

```
Detected HA member dead
```

**To manage individual cluster units**

This procedure describes how to log into the primary unit CLI and from there to connect to the CLI of subordinate cluster units. You log into the subordinate unit using the `ha_admin` administrator account. This built-in administrator account gives you read and write permission on the subordinate unit.

**1 Use SSH to connect to the cluster and log into the CLI.**

Connect to any cluster interface configured for SSH administrative access to log into the cluster.

You can also use a direct cable connection to log into the primary unit CLI. To do this you must know which unit is the primary unit.

**2 Enter the following command followed by a space and type a question mark (?):**

```
execute ha manage
```

The CLI displays a list of all the subordinate units in the cluster. Each cluster unit is numbered, starting at 1. The information displayed for each cluster unit includes the unit serial number and the host name of the unit.



- 3 Complete the command with the number of the subordinate unit to log into. For example, to log into subordinate unit 1, enter the following command:  

```
execute ha manage 1
```

Press Enter to connect to and log into the CLI of the selected subordinate unit. If this subordinate unit has a different host name, the CLI prompt changes to this host name. You can use CLI commands to manage this subordinate unit.
- 4 Enter the following command to return to the primary unit CLI:  

```
exit
```

You can use the `execute ha manage` command to log into the CLI of any of the other subordinate units in the cluster.

## SNMP

You can configure the FortiGate SNMP agent to report system information and send traps (alarms or event messages) to SNMP managers. Using an SNMP manager, you can access SNMP traps and data from any FortiGate interface or VLAN subinterface configured for SNMP management access.

The FortiGate SNMP implementation is read-only. SNMP v1 and v2c compliant SNMP managers have read-only access to FortiGate system information and can receive FortiGate traps. To monitor FortiGate system information and receive FortiGate traps you must compile Fortinet proprietary MIBs as well as Fortinet-supported standard MIBs into your SNMP manager.

RFC support includes support for most of RFC 2665 (Ethernet-like MIB) and most of RFC 1213 (MIB II) (for more information, see [“FortiGate MIBs” on page 101](#)).

This section describes:

- [Configuring SNMP](#)
- [SNMP community](#)
- [FortiGate MIBs](#)
- [FortiGate traps](#)
- [Fortinet MIB fields](#)

### Configuring SNMP

Go to **System > Config > SNMP v1/v2c** to configure the SNMP agent.

Figure 33: Configuring SNMP

The screenshot shows the SNMP configuration page. At the top, the 'SNMP Agent' is checked and enabled. Below it are text input fields for 'Description' (FortiGate unit), 'Location' (Server Room), and 'Contact' (System Admin ext 345), followed by an 'Apply' button. A 'Communities' section contains a 'Create New' button and a table with the following data:

Name	Queries	Traps	Enable	
Community_1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

<b>SNMP Agent</b>	Enable the FortiGate SNMP agent.
<b>Description</b>	Enter descriptive information about the FortiGate unit. The description can be up to 35 characters long.
<b>Location</b>	Enter the physical location of the FortiGate unit. The system location description can be up to 35 characters long.
<b>Contact</b>	Enter the contact information for the person responsible for this FortiGate unit. The contact information can be up to 35 characters long.
<b>Apply</b>	Save changes made to the description, location, and contact information.
<b>Create New</b>	Select Create New to add a new SNMP community.
<b>Communities</b>	The list of SNMP communities added to the FortiGate configuration. You can add up to 3 communities.
<b>Name</b>	The name of the SNMP community.
<b>Queries</b>	The status of SNMP queries for each SNMP community. The query status can be enabled or disabled.
<b>Traps</b>	The status of SNMP traps for each SNMP community. The trap status can be enabled or disabled.
<b>Enable</b>	Select Enable to activate an SNMP community.
<b>Delete icon</b>	Select Delete to remove an SNMP community.
<b>Edit/View icon</b>	View or modify an SNMP community.

## SNMP community

An SNMP community is a grouping of equipment for network administration purposes. Add SNMP communities so that SNMP managers can connect to the FortiGate unit to view system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiGate unit for a different set of events. You can also add the IP addresses of up to 8 SNMP managers to each community.

Figure 34: SNMP community options (part 1)

**New SNMP Community**

Community Name

**Hosts:**

IP Address	Interface	Delete
<input type="text" value="192.168.22.34"/>	<input type="text" value="internal"/>	
<input type="text" value="64.23.78.90"/>	<input type="text" value="external"/>	

**Add**

**Queries:**

Protocol	Port	Enable
v1	<input type="text" value="161"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="161"/>	<input checked="" type="checkbox"/>

**Traps:**

Protocol	Local	Remote	Enable
v1	<input type="text" value="162"/>	<input type="text" value="162"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="162"/>	<input type="text" value="162"/>	<input checked="" type="checkbox"/>

Figure 35: SNMP community options (part 2)

SNMP Event	Enable
CPU Overusage	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
Log disk space low	<input checked="" type="checkbox"/>
HA cluster status changed	<input checked="" type="checkbox"/>
Interface IP changed	<input checked="" type="checkbox"/>
Virus detected	<input checked="" type="checkbox"/>
Port scan detected	<input checked="" type="checkbox"/>
SYN flood detected	<input checked="" type="checkbox"/>
VPN tunnel up	<input checked="" type="checkbox"/>
VPN tunnel down	<input checked="" type="checkbox"/>

**OK** **Cancel**

**Community Name** Enter a name to identify the SNMP community.

**Hosts** Identify the SNMP managers that can use the settings in this SNMP community to monitor the FortiGate unit.

**IP Address** The IP address of an SNMP manager that can use the settings in this SNMP community to monitor the FortiGate unit. You can also set the IP address to 0.0.0.0 so that any SNMP manager can use this SNMP community.

**Interface** Optionally select the name of the interface that this SNMP manager uses to connect to the FortiGate unit. You only have to select the interface if the SNMP manager is not on the same subnet as the FortiGate unit. This can occur if the SNMP manager is on the Internet or behind a router.

**Add** Select Add to add more SNMP managers. You can add up to 8 SNMP managers to a single community. Select the Delete icon to remove an SNMP manager.

<b>Queries</b>	Enter the Port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the FortiGate unit. Select the Enable check box to activate queries for each SNMP version.
<b>Traps</b>	Enter the Local and Remote port numbers (162 by default) that the FortiGate unit uses to send SNMP v1 and SNMP v2c traps to the SNMP managers in this community. Select the Enable check box to activate traps for each SNMP version.
<b>SNMP Event</b>	Enable each SNMP event for which the FortiGate unit should send traps to the SNMP managers in this community.

### To configure SNMP access to an interface in NAT/Route mode

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections. See [“To control administrative access to an interface” on page 57](#).

- 1 Go to **System > Network > Interface**.
- 2 Choose an interface that an SNMP manager connects to and select Edit.
- 3 For Administrative Access, select SNMP.
- 4 Select OK.

### To configure SNMP access to an interface in Transparent mode

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections. See [“To configure the management interface” on page 60](#).

- 1 Go to **System > Network > Management**.
- 2 Choose an interface that the SNMP manager connects to and select SNMP.
- 3 Select Apply.

### To enable SNMP and configure basic SNMP settings

- 1 Go to **System > Config > SNMP v1/v2c**.
- 2 Select the Enable check box to enable the FortiGate SNMP Agent.
- 3 Configure the following SNMP settings: Description, Location, and Contact.
- 4 Select Apply.
- 5 Add one or more SNMP communities.

### To add an SNMP community

- 1 Go to **System > Config > SNMP v1/v2c**.
- 2 Select Create New.
- 3 Enter a Community Name to identify the SNMP community.
- 4 Configure Hosts, Queries, Traps, and SNMP Events.
- 5 Select OK.

## FortiGate MIBs

The FortiGate SNMP agent supports FortiGate proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiGate unit configuration.

The FortiGate MIBs are listed in [Table 6](#). You can obtain these MIB files from Fortinet technical support. To be able to communicate with the SNMP agent, you must compile all of these MIBs into your SNMP manager.

Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIBs to this database. If the standard MIBs used by the Fortinet SNMP agent are already compiled into your SNMP manager you do not have to compile them again.

**Table 6: FortiGate MIBs**

MIB file name or RFC	Description
<b>fortinet.2.80.mib</b>	The Fortinet MIB is a proprietary MIB that includes detailed FortiGate system configuration information. Add this MIB to your SNMP manager to monitor all FortiGate configuration settings. For more information about FortiGate MIB fields, see <a href="#">“FortiGate MIBs” on page 101</a> .
<b>fortinet.trap.2.80.mib</b>	The Fortinet trap MIB is a proprietary MIB that is required for your SNMP manager to receive traps from the FortiGate SNMP agent. For more information about FortiGate traps, see <a href="#">“FortiGate traps” on page 101</a> .
<b>RFC-1213 (MIB II)</b>	<p>The FortiGate SNMP agent supports MIB II groups with the following exceptions.</p> <p>No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).</p> <p>Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all FortiGate traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.</p>
<b>RFC-2665 (Ethernet-like MIB)</b>	<p>The FortiGate SNMP agent supports Ethernet-like MIB information with the following exception.</p> <p>No support for the dot3Tests and dot3Errors groups.</p>

## FortiGate traps

The FortiGate agent can send traps to SNMP managers that you have added to SNMP communities. For SNMP managers to receive traps, you must load and compile the Fortinet trap MIB (file name `fortinet.trap.2.80.mib`) onto the SNMP manager.

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

**Table 7: Generic FortiGate traps**

Trap message	Description
ColdStart WarmStart LinkUp LinkDown	Standard traps as described in RFC 1215.

**Table 8: FortiGate system traps**

Trap message	Description
CPU usage high (SysCpuHigh)	CPU usage exceeds 90%.
Disk low	On a FortiGate unit with a hard drive, hard drive usage exceeds 90%.
<FortiGate_serial_no> <interface_name>	The configuration of an interface of a FortiGate unit changes. The trap message includes the name of the interface and the serial number of the FortiGate unit.
HA state	HA state changes. The trap message includes the previous state, the new state and a flag indicating whether the unit is the master.
HA switch	The primary unit in an HA cluster fails and is replaced with a new primary unit.
Memory low (SysMemLow)	Memory usage exceeds 90%.
The <interface_name> Interface IP is changed to <new_IP> (Serial No.: <FortiGate_serial_no> (IntfIpChange)	The IP address of an interface of a FortiGate unit changes. The trap message includes the name of the interface, the new IP address of the interface, and the serial number of the FortiGate unit. This trap can be used to track interface IP address changes for interfaces configured with dynamic IP addresses set using DHCP or PPPoE.

**Table 9: FortiGate VPN traps**

Trap message	Description
VPN tunnel is up (VpnTunnelUp)	An IPSec VPN tunnel starts up and begins processing network traffic.
VPN tunnel down (VpnTunnelDown)	An IPSec VPN tunnel shuts down.

**Table 10: FortiGate IPS traps**

Trap message	Description
Syn flood attack. (IdsSynFlood)	NIDS attack prevention detects and provides protection from a syn flood attack.
Port scan attack. (IdsPortScan)	NIDS attack prevention detects and provides protection from a port scan attack.

**Table 11: FortiGate antivirus traps**

Trap message	Description
Virus detected (AvVirus)	The FortiGate unit detects a virus and removes the infected file from an HTTP or FTP download or from an email message.

**Table 12: FortiGate logging traps**

Trap message	Description
Log full (SysLogFull)	On a FortiGate unit with a hard drive, hard drive usage exceeds 90%. On a FortiGate unit without a hard drive, log to memory usage has exceeds 90%.

**Table 13: FortiGate HA traps**

Trap message	Description
Primary unit switch (HaSwitch)	The different unit in the HA cluster became the primary unit.

## Fortinet MIB fields

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

**Table 14: System MIB fields**

MIB field	Description
<b>model</b>	FortiGate model number, for example, 400 for the FortiGate-400.
<b>serial</b>	FortiGate unit serial number.
<b>version</b>	The firmware version currently running on the FortiGate unit.
<b>versionAv</b>	The antivirus definition version installed on the FortiGate unit.
<b>versionNids</b>	The attack definition version installed on the FortiGate unit.
<b>haMode</b>	The current FortiGate High-Availability (HA) mode (standalone, A-A, A-P)
<b>opMode</b>	The FortiGate unit operation mode (NAT or Transparent).
<b>cpuUsage</b>	The current CPU usage (as a percent).
<b>memUsage</b>	The current memory utilization (in MB).
<b>sesCount</b>	The current IP session count.

Table 15: HA MIB fields

MIB field	Description
<b>groupid</b>	HA group ID.
<b>priority</b>	The clustering priority of the individual FortiGate unit in a cluster.
<b>override</b>	The master-override setting (enable or disable) for an individual FortiGate unit in a cluster.
<b>autoSync</b>	Auto config synchronization flag.
<b>schedule</b>	Load balancing schedule for A-A mode.
<b>stats</b>	Statistics for all of the units in the HA cluster.
<b>index</b>	The index number of the FortiGate unit.
<b>serial</b>	The FortiGate unit serial number.
<b>cpuUsage</b>	The current FortiGate unit CPU usage as a percent.
<b>memUsage</b>	The current FortiGate unit memory usage (in MB).
<b>netUsage</b>	The current FortiGate unit network utilization (in Mbps).
<b>sesCount</b>	The number of active sessions being processed by the FortiGate unit.
<b>pktCount</b>	The number of packets processed by the FortiGate unit.
<b>byteCount</b>	The number of bytes processed by the FortiGate unit
<b>idsCount</b>	The number of attacks detected by the IPS running on the FortiGate unit in the last 20 hours.
<b>avCount</b>	The number of viruses detected by the antivirus system running on the FortiGate unit in the last 20 hours.

Table 16: Administrator accounts

MIB field	Description
<b>index</b>	The index number of the administrator account added to the FortiGate unit.
<b>name</b>	The user name of an administrator account added to the FortiGate unit.
<b>addr</b>	Up to three trusted host IP addresses for the administrator account.
<b>mask</b>	Up to three trusted host netmasks for the administrator account.
<b>perm</b>	The access profile assigned to the account.

Table 17: Local users

MIB field	Description
<b>index</b>	The index number of the local user added to the FortiGate unit.
<b>name</b>	The user name of the local user added to the FortiGate unit.
<b>auth</b>	The authentication type of for the local user. Can be password, LDAP, or RADIUS.
<b>state</b>	Whether the local user is enabled or disable.



Table 18: Virtual domains

MIB field	Description
<b>index</b>	The index number virtual domain added to the FortiGate unit.
<b>name</b>	The name of the virtual domain added to the FortiGate unit. Each FortiGate unit includes at least one virtual domain named root.
<b>auth</b>	The authentication type of for the local user. Can be password, LDAP, or RADIUS.
<b>state</b>	Whether the local user is enabled or disable.

Table 19: Active IP sessions










MIB field	Description
<b>index</b>	The index number of the active IP session.
<b>proto</b>	The IP protocol (TCP, UDP, ICMP, and so on) of the IP session.
<b>fromAddr</b>	The source IP address of the active IP session.
<b>fromPort</b>	The source port of the active IP session.
<b>toPort</b>	The destination IP address of the active IP session.
<b>toAddr</b>	The destination port of the active IP session.
<b>expiry</b>	The expiry time or time-to-live in seconds for the session.

## Replacement messages

Change replacement messages to customize alert email and information that the FortiGate unit adds to content streams such as email messages, web pages, and FTP sessions. The FortiGate unit adds replacement messages to a variety of content streams. For example, if a virus is found in an email message, the file is removed from the email and replaced with a replacement message. The same applies to pages blocked by web filtering and email blocked by spam filtering.

## Replacement messages list

Figure 36: Replacement messages list

Name	Description	
▶ <b>Mail</b>	Replacement for invalid mail service.	
▼ <b>HTTP</b>	Replacement for invalid http service.	
virus message	Replacement for infected files on the web.	
file block message	Replacement for blocked files on the web.	
oversized file message	Replacement for oversized files on the web.	
banned word message	Replacement for web pages containing banned words.	
URL block message	Replacement for blocked URLs.	
▼ <b>FTP</b>	Replacement for invalid ftp service.	
virus message	Replacement for infected FTP downloads or uploads.	
blocked message	Replacement for infected FTP downloads or uploads.	
oversized message	Replacement for oversized FTP downloads or uploads.	
▶ <b>Alert Mail</b>	Replacement for alert email.	
▶ <b>Spam</b>	Replacement for invalid smtp service.	
▼ <b>Category block</b>	Replacement for url blocked by category.	
URL block message	Category block message.	

**Name** The type of replacement message. You can change messages added to email, web pages in http traffic, messages that are displayed to ftp users, alert mail messages, messages added to smtp email, and messages added to web pages blocked by web filter category blocking.

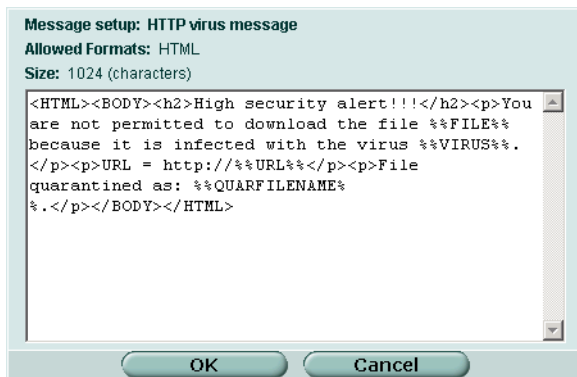
**Description** Description of the replacement message type. The web-based manager describes where each replacement message is used by the FortiGate unit. Edit/View icon. Select to change a replacement message.

### To change a replacement message

- 1 Go to **System > Config > Replacement Messages**.
- 2 Select the category of replacement message to edit by clicking on the blue triangle for that category.
- 3 For the replacement message that you want to change, select Edit.
- 4 Edit the content of the message.

## Changing replacement messages

Figure 37: Sample HTTP virus replacement message



Replacement messages can be text or HTML messages. You can add HTML code to HTML messages. In addition, replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message. [Table 20](#) lists the replacement message tags that you can add.

Table 20: Replacement message tags

Tag	Description
%%FILE%%	The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages.
%%VIRUS%%	The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used virus messages
%%QUARFILENAME%%	The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk.
%%URL%%	The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked.
%%CRITICAL_EVENT%%	Added to alert email critical event email messages. %%CRITICAL_EVENT%% is replaced with the critical event message that triggered the alert email.
%%PROTOCOL%%	The protocol (http, ftp, pop3, imap, or smtp) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages.
%%SOURCE_IP%%	The IP address of the request originator who would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed.
%%DEST_IP%%	The IP address of the request destination from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of web page that sent the virus.

**Table 20: Replacement message tags (Continued)**

Tag	Description
%%EMAIL_FROM%%	The email address of the sender of the message from which the file was removed.
%%EMAIL_TO%%	The email address of the intended receiver of the message from which the file was removed.
%%NIDSEVENT%%	The IPS attack message. %%NIDSEVENT%% is added to alert email intrusion messages.
%%SERVICE%%	The name of the web filtering service.
%%CATEGORY%%	The name of the content category of the web site.
%%FORTINET%%	The Fortinet logo.

## FortiManager

Configure the FortiGate unit for IPSec communication between the FortiGate unit and a FortiManager server. When you enable this feature, all communication between the FortiGate unit and the FortiManager server takes place using VPN.

**Figure 38: FortiManager configuration**

**Enable FortiManager** Enable secure IPSec VPN communication between the FortiGate unit and a FortiManager Server.

**FortiManager ID** The remote ID of the FortiManager IPSec tunnel.

**FortiManager IP** The IP Address of the FortiManager Server.

# System administration

When the FortiGate unit is first installed, it is configured with a single administrator account with the user name admin. From this administrator account, you can add and edit administrator accounts. You can also control the access level of each of these administrator accounts and control the IP address from which the administrator account can connect to the FortiGate unit.

Each administrator account belongs to an access profile. You can create access profiles that deny access to or allow read only, write only, or both read and write access to the following FortiGate features.

<b>System Configuration</b>	Can access the system status, interface, virtual domain, HA, routing, option, SNMP, time, and replacement message features.
<b>Log &amp; Report</b>	Can access the log setting, and log message features.
<b>Security Policy</b>	Can access the firewall, VPN, IPS, and antivirus features.
<b>Auth Users</b>	Can access the authorized users feature.
<b>Admin Users</b>	Can access the administrative users feature.
<b>FortiProtect Update</b>	Can access the update options feature.
<b>System Shutdown</b>	Can access the system shutdown, and system reboot functions.

This chapter describes:













- [Administrators](#)
- [Access profiles](#)

## Administrators

Use the admin account or an account with system configuration read and write privileges to add new administrator accounts and control their permission levels.

## Administrators list

Figure 39: Administrators list

Create New			
Name	Trusted hosts	Permission	
admin	0.0.0.0/0	prof_admin	  
Full_Privelege	192.168.110.100/32	prof_admin	  
Statistics	192.168.110.0/24	Log_only	  
Resources	192.168.50.0/24	User_manage	  

- Create New** Add an administrator account.
- Name** The login name for an administrator account.
- Trusted hosts** The trusted host IP address and netmask from which the administrator can log in.
- Permission** The permission profile for the administrator.  
The Delete, Edit/View, or Change Password icon.  
The admin administrator account cannot be deleted.

## Administrators options

Figure 40: Administrator account configuration

**New Administrator**

Administrator

Password

Confirm Password

Trusted Host #1  /

Trusted Host #2  /

Trusted Host #3  /

Access Profile


- Administrator** Enter the login name for the administrator account.
- Password** Type a password for the administrator account.  
For improved security, the password should be at least 6 characters long.
- Confirm Password** Type the password for the administrator account a second time to confirm that you have typed it correctly.
- Trusted Host #1** Optionally, type the trusted host IP address and netmask from which the administrator can log in to the FortiGate unit. You can specify up to three trusted hosts.
- Trusted Host #2**
- Trusted Host #3** Setting trusted hosts for all of your administrators can enhance the security of your system. For more information, see [“Using trusted hosts” on page 111](#).
- Access Profile** The access profile for the administrator. For more information on access profiles, see [“Access profile list” on page 112](#).

### To configure an administrator account

- 1 Go to **System > Admin > Administrators**.
- 2 Select Create New to add an administrator account or select the Edit icon to make changes to an existing administrator account.

- 3 Type a login name for the administrator account.
- 4 Type and confirm a password for the administrator account.
- 5 Optionally type a Trusted Host IP address and netmask from which the administrator can log into the web-based manager.
- 6 Select the access profile for the administrator.
- 7 Select OK.

**Figure 41: Change an administrator password**



The image shows a dialog box titled "Edit Password: Statistics". It has two input fields: "New Password" and "Confirm Password", both containing seven dots. Below the fields are two buttons: "OK" and "Cancel".

#### To change an administrator password

- 1 Go to **System > Admin > Administrators**.
- 2 Select the Change Password icon next to the administrator account you want to change the password for.
- 3 Enter and confirm the new password.
- 4 Select OK.

#### Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiGate unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

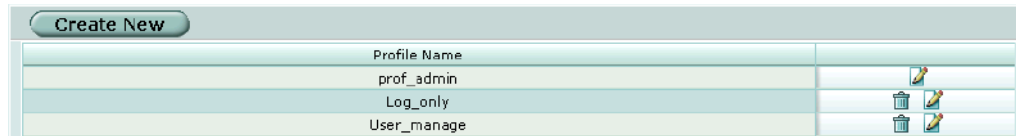
The trusted hosts you define apply both to the web-based manager and to the CLI when accessed through telnet or SSH. CLI access through the console connector is not affected.

## Access profiles

Go to **System > Admin > Access Profile** to add access profiles for FortiGate administrators. Each administrator account belongs to an access profile. You can create access profiles that deny access to or allow read only, write only, or both read and write access to FortiGate features.

## Access profile list

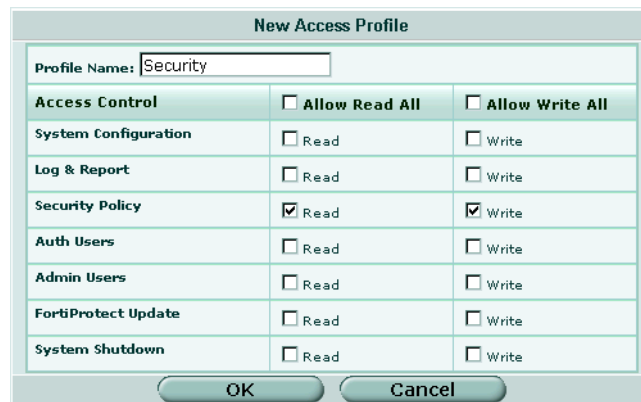
Figure 42: Access profile list



- Create New** Add a new access profile.
- Profile Name** The name of the access profile.  
The Delete, and Edit icons.  
You cannot delete the prof\_admin access profile.

## Access profile options

Figure 43: Access profile option



- Profile Name** Enter the name of the access profile.
- Access Control** Access Control lists the items that can be controlled by the access profile.
- Allow Read All** Select Allow Read All to give an administrator read privilege on all the items under Access Control.
- Allow Write All** Select Allow Write All to give an administrator write privilege on all the items under Access Control.
- System Configuration** Allow or deny access to the system status, interface, virtual domain, HA, routing, option, SNMP, time, and replacement message features.
- Log & Report** Allow or deny access to the log setting, log access, and alert email features.
- Security Policy** Allow or deny access to the firewall, VPN, IPS, and antivirus features.
- Auth Users** Allow or deny access to the authorized users feature.
- Admin Users** Allow or deny access to the administrative users feature.
- FortiProtect Update** Allow or deny access to the FortiProtect Distribution Network update feature.
- System Shutdown** Allow or deny access to the system shutdown and reboot functionality.



**To configure an access profile**

- 1** Go to **System > Admin > Access Profile**.
- 2** Select Create New to add an access profile, or select the edit icon to edit an existing access profile.
- 3** Enter a name for the access profile.
- 4** Select or clear the Access Control check boxes as required.
- 5** Select OK.




























## System maintenance

Use the web-based manager to maintain the FortiGate unit.

### Backup and restore

You can back up system configuration, VPN certificate, web and spam filtering files to the management computer. You can also restore system configuration, VPN certificate, web and spam filtering files from previously downloaded backup files.

**Figure 44: Backup and restore list**

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

**Category** The list of files that can be backed up and restored.

**Latest Backup** The date and time of the last backup.

The Restore/Upload, Backup and Reset to factory default icons.

**All Configuration Files** Restore or back up all the configuration files.

**System settings**

<b>System Configuration</b>	Restore or back up the FortiGate system configuration file. Reset the FortiGate unit to factory defaults. This procedure deletes all changes that you have made to the FortiGate configuration and reverts the system to its original configuration, including resetting interface addresses. This procedure does not change the firmware version or the antivirus or attack definitions.
<b>Debug Log</b>	Download debug log.
<b>Web Filtering</b>	
<b>Web Content Block</b>	Restore or back up the Web Content Block list.
<b>Web URL Block List</b>	Restore or back up the Web URL Block list.
<b>Web URL Exempt List</b>	Restore or back up the Web URL Exempt list.
<b>Spam Filtering</b>	
<b>IP Address</b>	Restore or back up the spam filter IP Address list.
<b>RBL &amp; ORDBL</b>	Restore or back up the spam filter RBL and ORDBL list.
<b>Email Address</b>	Restore or back up the spam filter Email Address list.
<b>MIME Headers</b>	Restore or back up the spam filter MIME Headers list.
<b>Banned Word</b>	Restore or back up the spam filter Banned word list.
<b>IPS Signatures</b>	
<b>IPS User-Defined Signatures</b>	Upload or download IPS signatures.
<b>VPN certificates</b>	
<b>All Certificates</b>	Restore or back up all VPN certificates in a single password-protected file. See <a href="#">“To restore VPN certificates”</a> and <a href="#">“To back up VPN certificates”</a> on page 117.

## Backing up and Restoring

### To back up all configuration files

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 For All Configuration Files, select the Backup icon.
- 3 Enter a password.
- 4 Select OK .
- 5 Save the file.

### To restore all configuration files

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 For All Configuration Files, select the Restore icon.
- 3 Enter the password you used when backing up All Configuration Files.
- 4 Enter the path and filename of the configuration file, or select Browse and locate the file.

- 5 Select OK to restore all configuration files to the FortiGate unit. The FortiGate unit restarts, loading the new configuration files.
- 6 Reconnect to the web-based manager and review your configuration to confirm that the uploaded configuration files have taken effect.

#### To back up individual categories

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 Select the Backup icon for the type of file you want to back up.
- 3 Save the file.

#### To restore individual categories

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 Select the Restore icon for the type of file you want to restore.
- 3 Enter the path and filename of the file, or select Browse and locate the file.
- 4 Select OK.

If you restore the system configuration, the FortiGate unit restarts, loading the new system settings. You should then reconnect to the web-based manager and review your configuration to confirm that the uploaded system settings have taken effect.

- 5 Select Return. (This step does not apply if you restore the system configuration.)

#### To back up VPN certificates

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 For VPN Certificates, All Certificates, select the Backup icon.
- 3 Enter a password and select OK.  
Retain the password. You will need it to restore the certificates.
- 4 Save the file.

#### To restore VPN certificates

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 For VPN Certificates, All Certificates, select the Restore icon.
- 3 Enter the password used when creating the backup file.
- 4 Enter the path and filename of the backup file, or select Browse and locate the file.
- 5 Select OK.

## Update center

You can configure the FortiGate unit to connect to the FortiProtect Distribution Network (FDN) to update the antivirus (including grayware), Spam Filter and attack definitions and engines.

Before the FortiGate unit can receive antivirus and attack updates, it must be able to connect to the FortiProtect Distribution Network (FDN). The FortiGate unit uses HTTPS on port 8890 to connect to the FDN. The FortiGate unit must be able to route packets to the Internet using port 8890. For information about configuring scheduled updates, see [“To enable scheduled updates” on page 121](#).

You can also configure the FortiGate unit to allow push updates. Push updates are provided to the FortiGate unit from the FDN using HTTPS on UDP port 9443. To receive push updates, the FDN must be able to route packets to the FortiGate unit using UDP port 9443. For information about configuring push updates, see [“To enable push updates” on page 123](#).

The FDN is a world-wide network of FortiProtect Distribution Servers (FDSs). When the FortiGate unit connects to the FDN it connects to the nearest FDS. To do this, all FortiGate units are programmed with a list of FDS addresses sorted by nearest time zone according to the time zone configured for the FortiGate unit.

The FortiGate unit supports the following antivirus and attack definition update features:

- User-initiated updates from the FDN,
- Hourly, daily, or weekly scheduled antivirus and attack definition and antivirus engine updates from the FDN,
- Push updates from the FDN,
- Update status including version numbers, expiry dates, and update dates and times,
- Push updates through a NAT device.

To receive scheduled updates and push updates, you must register the FortiGate unit on the Fortinet support web page.

Figure 45: Update center

**FortiProtect Distribution Network** Unknown Refresh

**Push Update** not available

Use override server address

Update	Version	Expiry date	Last update attempt	Last Update Status
Anti Virus Engine	1.061	n/a	n/a	Installed updates
Anti Virus Definition	4.479	n/a	n/a	Installed updates
Attack Definition	2.135	n/a	n/a	Installed updates
IPS Attack Engine	1.000	n/a	n/a	Installed updates
Anti Spam Definition	0.000	n/a	n/a	Installed updates

**Allow Push Update**

Use override push IP  Port

**Scheduled Update**

Every  (hour)

Daily:  (hour)

Weekly:  (day)  (hour)

Apply Update Now

### FortiProtect Distribution Network

The status of the connection to the FortiProtect Distribution Network (FDN). A green indicator means that the FortiGate unit can connect to the FDN. You can configure the FortiGate unit for scheduled updates. See [“To enable scheduled updates” on page 121](#).

A red-yellow flashing indicator means that the FortiGate unit cannot connect to the FDN. Check your configuration. For example, you may need to add routes to the FortiGate routing table or configure your network to allow the FortiGate unit to use HTTPS on port 8890 to connect to the Internet. You may also have to connect to an override FortiProtect server to receive updates. See [“To add an override server” on page 121](#).

### Push Update

A green indicator means that the FDN can connect to the FortiGate unit to send push updates. You can configure the FortiGate unit to receive push updates. See [“To enable push updates” on page 123](#).

A red-yellow flashing indicator means that the FDN cannot connect to the FortiGate unit to send push updates. Push updates may not be available if you have not registered the FortiGate unit (see [“To register a FortiGate unit” on page 128](#)), if there is a NAT device installed between the FortiGate unit and the FDN (see [“Enabling push updates through a NAT device” on page 124](#)), or if your FortiGate unit connects to the Internet using a proxy server (see [“To enable scheduled updates through a proxy server” on page 122](#)).

### Refresh

When you select Refresh, the FortiGate unit tests its connection to the FDN. The test results are displayed at the top of the System Update page.

### Use override server address

If you cannot connect to the FDN or if your organization provides antivirus and attack updates using their own FortiProtect server, you can configure an override server.

Select the Use override server address check box and enter the IP address of a FortiProtect server.

If after applying the override server address, the FortiProtect Distribution Network setting changes to available, the FortiGate unit has successfully connected to the override server. If the FortiProtect Distribution Network stays set to not available, the FortiGate unit cannot connect to the override server. Check the FortiGate configuration and the network configuration to make sure you can connect to the override FortiProtect server from the FortiGate unit.

### Update

The antivirus (including grayware), Spam filter, and attack definitions and engines for which update information is displayed.

<b>Version</b>	The version numbers of the definition files and engines currently installed on the FortiGate unit.
<b>Expiry date</b>	The expiry date of your license for definition and engine updates.
<b>Last update attempt</b>	The date and time on which the FortiGate unit last attempted to download definition and engine updates.
<b>Last update status</b>	The result of the last update attempt. No updates means the last update attempt was successful but no new updates were available. Update succeeded or similar messages mean the last update attempt was successful and new updates were installed. Other messages can indicate that the FortiGate was not able to connect to the FDN and other error conditions.
<b>Allow Push Update</b>	Select this check box to allow automatic updates of the FortiGate unit.
<b>Use override push IP</b>	Select this check box and enter the override IP address and port number. Override push IP addresses and ports are used when there is a NAT device between the FortiGate Unit and the FDN. The FortiGate unit sends the override push IP address and Port to the FDN. The FDN will now use this IP address and port for push updates to the FortiGate unit on the internal network. If the External IP Address or External Service Port change, add the changes to the Use override push configuration and select Apply to update the push information on the FDN. For more information, see <a href="#">"Enabling push updates through a NAT device" on page 124.</a>
<b>Scheduled Update</b>	Select this check box to enable scheduled updates.
<b>Every</b>	Attempt to update once every 1 to 23 hours. Select the number of hours between each update request.
<b>Daily</b>	Attempt to update once a day. You can specify the hour of the day to check for updates. The update attempt occurs at a randomly determined time within the selected hour.
<b>Weekly</b>	Attempt to update once a week. You can specify the day of the week and the hour of the day to check for updates. The update attempt occurs at a randomly determined time within the selected hour.
<b>Update Now</b>	Select Update Now to manually initiate an update.
<b>Apply</b>	Select Apply to save update settings.

## Updating antivirus and attack definitions

Use the following procedures to configure the FortiGate unit to connect to the FortiProtect Distribution Network (FDN) to update the antivirus (including grayware) definitions, attack definitions and engines.

### To make sure the FortiGate unit can connect to the FDN

- 1 Go to **System > Config > Time** and make sure the time zone is set to the time zone for the region in which your FortiGate unit is located.
- 2 Go to **System > Maintenance > Update center**.
- 3 Select Refresh.  
The FortiGate unit tests its connection to the FDN. The test results are displayed at the top of the System Update page.

### To update antivirus and attack definitions

- 1 Go to **System > Maintenance > Update center**.



- 2 Select Update Now to update the antivirus and attack definitions and engines.

If the connection to the FDN or override server is successful, the web-based manager displays a message similar to the following:

Your update request has been sent. Your database will be updated in a few minutes. Please check your update page for the status of the update.

After a few minutes, if an update is available, the System Update Center page lists new version information for antivirus definitions, the antivirus engine, attack definitions or the attack engine. The System Status page also displays new dates and version numbers for antivirus and attack definitions. Messages are recorded to the event log indicating whether the update was successful or not.



**Note:** Updating antivirus and attack definitions can cause a very short disruption in traffic currently being scanned while the FortiGate unit applies the new signature database. To minimize this possibility, schedule updates for times of light traffic.

#### To enable scheduled updates

- 1 Go to **System > Maintenance > Update center**.
- 2 Select the Scheduled Update check box.
- 3 Select one of the following to check for and download updates.

**Every** Once every 1 to 23 hours. Select the number of hours and minutes between each update request.

**Daily** Once a day. You can specify the time of day to check for updates.

**Weekly** Once a week. You can specify the day of the week and the time of day to check for updates.

- 4 Select Apply.

The FortiGate unit starts the next scheduled update according to the new update schedule.

Whenever the FortiGate unit runs a scheduled update, the event is recorded in the FortiGate event log.

#### To add an override server

If you cannot connect to the FDN, or if your organization provides antivirus and attack updates using their own FortiProtect server, you can use the following procedure to add the IP address of an override FortiProtect server.

- 1 Go to **System > Maintenance > Update center**.
- 2 Select the Use override server address check box.
- 3 Type the fully qualified domain name or IP address of a FortiProtect server.

#### 4 Select Apply.

The FortiGate unit tests the connection to the override server.

If the FortiProtect Distribution Network setting changes to available, the FortiGate unit has successfully connected to the override server.

If the FortiProtect Distribution Network stays set to not available, the FortiGate unit cannot connect to the override server. Check the FortiGate configuration and network configuration for settings that would prevent the FortiGate unit from connecting to the override FortiProtect server.

#### To enable scheduled updates through a proxy server

If your FortiGate unit must connect to the Internet through a proxy server, you can use the `config system autoupdate tunneling` command to allow the FortiGate unit to connect (or tunnel) to the FDN using the proxy server. Using this command you can specify the IP address and port of the proxy server. As well, if the proxy server requires authentication, you can add the user name and password required for the proxy server to the autoupdate configuration. The full syntax for enabling updates through a proxy server is:

```
config system autoupdate tunneling
  set address <proxy-address_ip>
  set port <proxy-port>
  set username <username_str>
  set password <password_str>
  set status enable
end
```

For example, if the IP address of the proxy server is 67.35.50.34, its port is 8080, the user name is proxy\_user and the password is proxy\_pwd, enter the following command:

```
config system autoupdate tunneling
  set address 67.35.50.34
  set port 8080
  set username proxy_user
  set password proxy_pwd
  set status enable
end
```

For more information about the `config system autoupdate tunneling` command, see the *FortiGate CLI Reference Guide*.

The FortiGate unit connects to the proxy server using the HTTP CONNECT method, as described in RFC 2616. The FortiGate unit sends an HTTP CONNECT request to the proxy server (optionally with authentication information) specifying the IP address and port required to connect to the FDN. The proxy server establishes the connection to the FDN and passes information between the FortiGate unit and the FDN.

The CONNECT method is used mostly for tunneling SSL traffic. Some proxy servers do not allow the CONNECT to connect to any port; they restrict the allowed ports to the well known ports for HTTPS and perhaps some other similar services. Because FortiGate autoupdates use HTTPS on port 8890 to connect to the FDN, your proxy server might have to be configured to allow connections on this port.

There are no special tunneling requirements if you have configured an override server address to connect to the FDN.

## Enabling push updates

The FDN can push updates to FortiGate units to provide the fastest possible response to critical situations. You must register the FortiGate unit before it can receive push updates. See [“To register a FortiGate unit” on page 128](#).

When you configure a FortiGate unit to allow push updates, the FortiGate unit sends a SETUP message to the FDN. The next time a new antivirus engine, new antivirus definitions, new attack definitions or new attack engine are released, the FDN notifies all FortiGate units that are configured for push updates that a new update is available. Within 60 seconds of receiving a push notification, the FortiGate unit requests an update from the FDN.



**Note:** Push updates are not supported if the FortiGate unit must use a proxy server to connect to the FDN. For more information, see [“To enable scheduled updates through a proxy server” on page 122](#).

When the network configuration permits, configuring push updates is recommended in addition to configuring scheduled updates. On average the FortiGate unit receives new updates sooner through push updates than if the FortiGate unit receives only scheduled updates. However, scheduled updates make sure that the FortiGate unit receives the latest updates.

Enabling push updates is not recommended as the only method for obtaining updates. The FortiGate unit might not receive the push notification. Also, when the FortiGate unit receives a push notification it makes only one attempt to connect to the FDN and download updates.

### To enable push updates

- 1 Go to **System > Maintenance > Update center**.
- 2 Select Allow Push Update.
- 3 Select Apply.

## Push updates when FortiGate IP addresses change

The SETUP message that the FortiGate unit sends when you enable push updates includes the IP address of the FortiGate interface that the FDN connects to. If your FortiGate unit is running in NAT/Route mode, the SETUP message includes the FortiGate external IP address. If your FortiGate unit is running in Transparent mode, the SETUP message includes the FortiGate management IP address. The FDN must be able to connect to this IP address for your FortiGate unit to be able to receive push update messages. If your FortiGate unit is behind a NAT device, see [“Enabling push updates through a NAT device” on page 124](#).

Whenever the external IP address of the FortiGate unit changes, the FortiGate unit sends a new SETUP message to notify the FDN of the address change. As long as the FortiGate unit sends this SETUP message and the FDN receives it, the FDN can maintain the most up-to-date external IP address for the FortiGate unit.

The FortiGate unit sends the SETUP message if you change the external IP address manually or if you have set the external interface addressing mode to DHCP or PPPoE and your DHCP or PPPoE server changes the IP address.

If you have redundant connections to the Internet, the FortiGate unit also sends the SETUP message when one Internet connection goes down and the FortiGate unit fails over to the other Internet connection.

In Transparent mode if you change the management IP address, the FortiGate unit also sends the SETUP message to notify the FDN of the address change.

## Enabling push updates through a NAT device

If the FDN can connect to the FortiGate unit only through a NAT device, you must configure port forwarding on the NAT device and add the port forwarding information to the push update configuration. Using port forwarding, the FDN connects to the FortiGate unit using either port 9443 or an override push port that you specify.



**Note:** You cannot receive push updates through a NAT device if the external IP address of the NAT device is dynamic (for example, set using PPPoE or DHCP).

### General procedure

Use the following steps to configure the FortiGate NAT device and the FortiGate unit on the internal network so that the FortiGate unit on the internal network can receive push updates:

- 1 Add a port forwarding virtual IP to the FortiGate NAT device.
- 2 Add a firewall policy to the FortiGate NAT device that includes the port forwarding virtual IP.
- 3 Configure the FortiGate unit on the internal network with an override push IP and port.



**Note:** Before completing the following procedure, you should register the internal network FortiGate unit so that it can receive push updates.

### To add a port forwarding virtual IP to the FortiGate NAT device

Configure a FortiGate NAT device to use port forwarding to forward push update connections from the FDN to a FortiGate unit on the internal network.

- 1 Go to **Firewall > Virtual IP**.
- 2 Select Create New.
- 3 Type a name for the virtual IP.
- 4 In the External Interface section, select the external interface that the FDN connects to.
- 5 In the Type section, select Port Forwarding.
- 6 In the External IP Address section, type the external IP address that the FDN connects to.
- 7 Type the External Service Port that the FDN connects to.

- 8 In the Map to IP section, type the IP address of the FortiGate unit on the internal network.  
If the FortiGate unit is operating in NAT/Route mode, enter the IP address of the external interface.  
If the FortiGate unit is operating in Transparent mode, enter the management IP address.
- 9 Set the Map to Port to 9443.
- 10 Select OK.

#### To add a firewall policy to the FortiGate NAT device

- 1 Add a new external to internal firewall policy.
- 2 Configure the policy with the following settings:

<b>Source</b>	External_All
<b>Destination</b>	The virtual IP added above.
<b>Schedule</b>	Always
<b>Service</b>	ANY
<b>Action</b>	Accept
<b>NAT</b>	Selected.

- 3 Select OK.

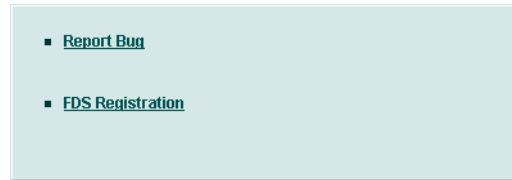
#### To configure the FortiGate unit on the internal network

- 1 Go to **System > Maintenance > Update center**.
- 2 Select the Allow Push Update check box.
- 3 Select the Use override push check box.
- 4 Set IP to the external IP address added to the virtual IP.
- 5 Set Port to the external service port added to the virtual IP.
- 6 Select Apply.  
The FortiGate unit sends the override push IP address and port to the FDN. The FDN now uses this IP address and port for push updates to the FortiGate unit on the internal network.  
If the external IP address or external service port changes, add the changes to the Use override push configuration and select Apply to update the push information on the FDN.
- 7 You can select Refresh to make sure that push updates work.  
Push Update changes to Available.

## Support

You can use the Support page to report problems with the FortiGate unit to Fortinet Support or to register your FortiGate unit with the FortiProtect Distribution Server (FDS).

Figure 46: Support



**Report Bug** Select Report Bug to submit problems with the FortiGate unit to Fortinet Support.

**FDS Registration** Select FDS Registration to register the FortiGate unit with FortiNet.

## Sending a bug report

Use the Report Bug form to send bug information to Fortinet support.

Figure 47: Bug report

 A screenshot of the 'Report Bug' form. The form has a title bar that says 'Report Bug'. Below the title bar are several input fields: 'First Name\*', 'Last Name\*', 'Company\*', 'Address\*', 'Contact Phone\*', 'Fax', and 'Email\*'. Below these is a large text area for 'Bug Description\*'. Underneath the text area are three radio button options: 'Send diagnostic information.', 'Send email by default mail-relay. Test', and 'Send email by customized mail-relay.'. Below the radio buttons are three input fields for 'SMTP Server', 'User Name', and 'Password'. There is also an 'Authentication' section with 'Yes' and 'No' radio buttons. At the bottom left, there is a note '\* - required'. At the bottom right, there are two buttons: 'Submit' and 'Cancel'.

**Contact Information** Enter the contact information so that FortiNet support can reply to your bug report. Items marked with an \* are required.

**Bug Description\*** Enter a description of the problem you have encountered with the FortiGate unit.

**Send diagnostic information** Send diagnostic information about the FortiGate unit, including its current configuration, to Fortinet for analysis.

**Send email by default mail-relay** Submit the bug report using the default mail relay.

**Test** Test the default mail relay.

<b>Send email by customized mail-relay</b>	Submit the bug report using a customized mail relay.
<b>SMTP Server</b>	The SMTP server to use for sending bug report email.
<b>User Name</b>	A valid user name on the specified SMTP server.
<b>Password</b>	If the SMTP server requires authentication, enter the password required.
<b>Authentication</b>	Select No if the SMTP server does not require authentication. Select Yes if the SMTP server does require authentication.

#### To report a bug

- 1 Go to **System > Maintenance > Support**.
- 2 Select Report Bug.
- 3 Fill out the Report Bug form.
- 4 Select Submit.

#### To configure a customized mail relay

- 1 Go to **System > Maintenance > Support**.
- 2 Select Report Bug.
- 3 Select Send email by customized mail-relay.
- 4 Enter the SMTP server information, user name, whether or not to use authentication, and the password if required.

## Registering a FortiGate unit

After purchasing and installing a new FortiGate unit, you can register the unit using the web-based manager by going to the System Update Support page, or by using a web browser to connect to <http://support.fortinet.com> and selecting Product Registration.

Registration consists of entering your contact information and the serial numbers of the FortiGate units that you or your organization purchased. You can register multiple FortiGate units in a single session without re-entering your contact information.

Once registration is completed, Fortinet sends a Support Login user name and password to your email address. You can use this user name and password to log on to the Fortinet support web site to:

- View your list of registered FortiGate units
- Register additional FortiGate units
- Add or change FortiCare Support Contract numbers for each FortiGate unit
- View and change registration information
- Download virus and attack definitions updates
- Download firmware upgrades
- Modify registration information after an RMA

Soon you will also be able to:

- Access Fortinet user documentation
- Access the Fortinet knowledge base

All registration information is stored in the Fortinet Customer Support database. This information is used to make sure that your registered FortiGate units can be kept up to date. All information is strictly confidential. Fortinet does not share this information with any third-party organizations for any reason.

Owners of a new FortiGate unit are entitled to 90 days of technical support services. To continue receiving support services after the 90-day expiry date, you must purchase a FortiCare Support Contract from an authorized Fortinet reseller or distributor. Different levels of service are available so you can purchase the support that you need. For maximum network protection, Fortinet strongly recommends that all customers purchase a service contract that covers antivirus and attack definition updates. See your Fortinet reseller or distributor for details of packages and pricing.

To activate the FortiCare Support Contract, you must register the FortiGate unit and add the FortiCare Support Contract number to the registration information. You can also register the FortiGate unit without purchasing a FortiCare Support Contract. In that case, when you purchase a FortiCare Support Contract you can update the registration information to add the support contract number.

A single FortiCare Support Contract can cover multiple FortiGate units. You must enter the same service contract number for each of the FortiGate models covered by the service contract.

### **To register a FortiGate unit**

Before registering a FortiGate unit, you require the following information:

- Your contact information including:
  - First and last name
  - Company name
  - Email address (Your Fortinet support login user name and password will be sent to this email address.)
  - Address
  - Contact phone number
- A security question and an answer to the security question.

This information is used for password recovery. The security question should be a simple question that only you know the answer to. The answer should not be easy to guess.
- The product model and serial number for each FortiGate unit that you want to register.

The serial number is located on a label on the bottom of the FortiGate unit.

You can view the Serial number from the web-based manager by going to System > Status.

The serial number is also available from the CLI using the `get system status` command.



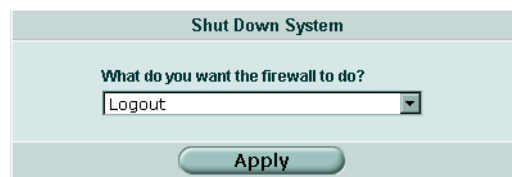
FortiCare Support Contract numbers, if you purchased FortiCare Support Contracts for the FortiGate units that you want to register.

- 1 Go to **System > Maintenance > Support**.
- 2 Select FDS Registration.
- 3 Enter your contact information on the product registration form.
- 4 Provide a security question and an answer to the security question.
- 5 Select the model number of the Product Model to register.
- 6 Enter the Serial Number of the FortiGate unit.
- 7 If you have purchased a FortiCare Support Contract for this FortiGate unit, enter the support contract number.
- 8 Select Finish.  
If you have not entered a FortiCare Support Contract number (SCN) you can return to the previous page to enter the number. If you do not have a FortiCare Support Contract, you can select Continue to complete the registration.  
If you have entered a support contract number, a real-time validation is performed to verify that the SCN information matches the FortiGate unit. If the information does not match you can try entering it again.  
A web page is displayed that contains detailed information about the Fortinet technical support services available to you for the registered FortiGate unit.
- 9 Your Fortinet support user name and password is sent to the email address provided with your contact information.

## Shutdown

You can use the Maintenance page to log out, restart and shut down the FortiGate unit.

**Figure 48: System shut down**



### To log out of the system

- 1 Go to **System > Maintenance > Shutdown**.
- 2 Select Logout.
- 3 Select Apply.  
The FortiGate unit logs out.

### To restart the system

- 1 Go to **System > Maintenance > Shutdown**.

- 2 Select Reboot.
- 3 Select Apply.  
The FortiGate unit restarts.

#### To shut down the system

You can restart the FortiGate unit after shutdown only by turning the power off and then on.

- 1 Go to **System > Maintenance > Shutdown**.
- 2 Select Shutdown.
- 3 Select Apply.  
The FortiGate unit shuts down and all traffic flow stops.

#### To reset the FortiGate unit to factory defaults

Use the following procedure to reset system settings to the values set at the factory. This procedure does not change the firmware version or the antivirus or attack definitions.



**Caution:** This procedure deletes all changes that you have made to the FortiGate configuration and reverts the system to its original configuration, including resetting interface addresses.

- 1 Go to **System > Maintenance > Shutdown**.
- 2 Select Reset to factory default.
- 3 Select Apply.  
The FortiGate unit restarts with the configuration that it had when it was first powered on.
- 4 Reconnect to the web-based manager and review the system configuration to confirm that it has been reset to the default settings.

# System virtual domain

FortiGate virtual domains provide multiple logical firewalls and routers in a single FortiGate unit. Using virtual domains, one FortiGate unit can provide exclusive firewall and routing services to multiple networks so that traffic from each network is effectively separated from every other network.

You can develop and manage interfaces, VLAN subinterfaces, zones, firewall policies, routing, and VPN configuration for each virtual domain separately. For these configuration settings, each virtual domain is functionally similar to a single FortiGate unit. This separation simplifies configuration because you do not have to manage as many routes or firewall policies at one time.

When a packet enters a virtual domain on the FortiGate unit, it is confined to that virtual domain. In a given domain, you can only create firewall policies for connections between VLAN subinterfaces or zones in the virtual domain. Packets never cross the virtual domain border.

The remainder of FortiGate functionality is shared between virtual domains. This means that there is one IPS configuration, one antivirus configuration, one web filter configuration, one protection profile configuration, and so on shared by all virtual domains. As well, virtual domains share firmware versions, antivirus and attack databases, and user databases. For a complete list of shared configuration settings, see [“Shared configuration settings” on page 133](#).

Virtual domains are functionally similar in NAT/Route and in Transparent mode. In both cases interfaces, VLAN subinterfaces, zones, firewall policies, routing, and VPN configurations are exclusive to each virtual domain and other configuration settings are shared. A major difference between NAT/Route and Transparent mode is that in Transparent mode, interfaces, and VLAN interfaces do not have IP addresses and routing is much simpler.

The FortiGate unit supports 2 virtual domains: root and one addition virtual domain.

This chapter describes:

- [Virtual domain properties](#)
- [Virtual domains](#)
- [Configuring virtual domains](#)

## Virtual domain properties

By default, each FortiGate unit runs a virtual domain named root. This virtual domain includes all of the FortiGate physical interfaces, VLAN subinterfaces, zones, firewall policies, routing settings, and VPN settings.

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

This process works the same way in NAT/Route and in Transparent mode.

### Exclusive virtual domain properties

The following configuration settings are exclusively part of a virtual domain and are not shared between virtual domains.

- System settings
  - Physical interfaces (see [“To add physical interfaces to a virtual domain” on page 136](#))
  - VLAN subinterfaces (see [“To add VLAN subinterfaces to a virtual domain” on page 137](#))
  - Zones (see [“To add zones to a virtual domain” on page 137](#))
  - Management IP (Transparent mode) (see [“To select a management virtual domain and add a management IP” on page 136](#))
- Routing configuration
  - Router configuration in NAT/Route mode (see [“To configure routing for a virtual domain in NAT/Route mode” on page 138](#))
  - Routing table configuration in Transparent mode (see [“To configure the routing table for a virtual domain in Transparent mode” on page 138](#))
- Firewall settings
  - Policies (see [“To add firewall policies to a virtual domain” on page 138](#))
  - Addresses (see [“To add firewall addresses to a virtual domain” on page 139](#))
  - Service groups
  - IP pools (are associated with an interface) (see [“To add IP pools to a virtual domain” on page 139](#))
  - Virtual IPs (are associated with an interface) (see [“To add Virtual IPs to a virtual domain” on page 139](#))
- VPN (see [“To configure VPN for a virtual domain” on page 140](#))
  - IPSec
  - PPTP
  - L2TP
  - Certificates

## Shared configuration settings

The following configuration settings are shared by all virtual domains. Even if you have configured multiple virtual domains, there are no changes to how you configure the following settings.

- Unit configuration
  - Host Name
  - Firmware Version
  - Antivirus Definitions and engine
  - Attack Definitions and engine
  - Serial Number
  - Operation Mode
- Network configuration
  - DNS settings
- DHCP configuration

DHCP settings are applied per interface no matter which virtual domain the interface has been added to
- System Config
  - Time
  - Options
  - HA
  - SNMP v1/v2c
  - Replacement messages
  - FortiManager configuration
- System Admin
  - Administrators
  - Access profiles
- System Maintenance
  - Update Center
- Firewall
  - Services (predefined and custom) but not service groups
  - Schedules
  - Protection Profiles
- Users and authentication
- IPS
- Antivirus
- Web filter
- Spam filter
- Log and report

## Administration and management

In addition to the global properties, virtual domains share a common administrative model. Administrators have access to all of the virtual domains on the FortiGate unit. Administrators logging into the CLI or web-based manager always log into the root domain and then must enter the virtual domain that they want to administer.

Management systems such as SNMP, logging, alert email, updates using the FDN, and setting system time using NTP use addresses and routing in the root virtual domain to communicate with the network and can only connect to network resources that can communicate with the root virtual domain.

You can select a different management virtual domain if you want these systems to communicate with network resources that can connect to a different virtual domain.

## Virtual domains

Go to **System > Virtual domain > Virtual domains** to view and add virtual domains.

**Figure 49: Virtual domain list**

Create New			
Current: root <a href="#">[change]</a>		Management: root <a href="#">[change]</a>	
Max Virtual Domains: 2			
Name	Current	Management	
root	✓	✓	
domain2			🗑️

**Create New** Add a new virtual domain.

**Current** The name of the current virtual domain. Select Change to choose a different domain. The default virtual domain is root.

**Management** The name of the virtual domain used for system management. Select Change to choose a different domain.

**Max. Virtual Domains** Shows the maximum number of virtual domains for this FortiGate unit.

**Name** The name of the virtual domain.

**Current** A check mark icon in this column indicates that this is the current domain.

**Management** A check mark icon in this column indicates that this is the domain used for system management.

Delete icon. Select to delete a virtual domain. You cannot delete the root virtual domain or a domain that is used for system management.

See the following procedures for configuring virtual domains:

- [To add VLAN subinterfaces to a virtual domain](#)
- [To view the interfaces in a virtual domain](#)
- [To add zones to a virtual domain](#)
- [To select a management virtual domain and add a management IP](#)
- [To configure routing for a virtual domain in NAT/Route mode](#)
- [To configure the routing table for a virtual domain in Transparent mode](#)
- [To add firewall policies to a virtual domain](#)
- [To add firewall addresses to a virtual domain](#)
- [To add IP pools to a virtual domain](#)
- [To add Virtual IPs to a virtual domain](#)
- [To configure VPN for a virtual domain](#)

## Adding a virtual domain

### To add a virtual domain

- 1 Go to **System > Virtual domain**.
- 2 Select Create New.
- 3 Enter a virtual domain Name.  
The virtual domain must not have the same name as a VLAN or zone.
- 4 Select OK.

## Selecting a virtual domain

The following procedure applies to NAT/Route and Transparent mode.

### To select a virtual domain to configure

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain to configure.
- 4 Select OK.

The footer of the web-based manager page displays the selected virtual domain name if the information and configuration options on the page are exclusive to the virtual domain. Otherwise, the footer displays "Virtual Domain: all". See ["Exclusive virtual domain properties"](#) on page 132.

## Selecting a management virtual domain

In NAT/Router mode, you select a virtual domain to be used for system management. In Transparent mode, you must also define a management IP. The interface that you want to use for management access must have Administrative Access enabled. See ["To control administrative access to an interface"](#) on page 57.

**To select a management virtual domain**

The following procedure applies to NAT/Route mode only.

- 1 Go to **System > Virtual Domain > Virtual Domains**.
- 2 Select Change beside the listed Management virtual domain.
- 3 Choose the management domain and select OK.



**Note:** You cannot delete a management virtual domain. You must first select a different domain for system management.

**To select a management virtual domain and add a management IP**

The following procedure applies to Transparent mode only.

- 1 Go to **System > Network > Management**.
- 2 Enter the Management IP/Netmask.
- 3 Enter the Default Gateway.
- 4 Select the Management Virtual Domain.
- 5 Select Apply.

The FortiGate unit displays the following message:

Management IP address was changed. Click here to redirect.

- 6 Click on the message to connect to the new Management IP.

## Configuring virtual domains

The following procedures explain how to configure virtual domains:

- [Adding interfaces, VLAN subinterfaces, and zones to a virtual domain](#)
- [Configuring routing for a virtual domain](#)
- [Configuring firewall policies for a virtual domain](#)
- [Configuring IPsec VPN for a virtual domain](#)

### Adding interfaces, VLAN subinterfaces, and zones to a virtual domain

**To add physical interfaces to a virtual domain**

A virtual domain must contain at least two interfaces. These can be physical interfaces or VLAN interfaces.

By default all physical interfaces are in the root virtual domain and the following procedure describes how to move a physical interface from one virtual domain to another. You cannot remove a physical interface from a virtual domain if firewall policies have been added for it. Delete the firewall policies or remove the interface from the firewall policies first. If the interface has been added to a zone, it is removed from the zone when you move it to a different virtual domain.

- 1 Go to **System > Network > Interface**.



- 2 Set Virtual domain to All or to the name of the virtual domain that currently contains the interface.
- 3 Select Edit for the physical interface you want to move.
- 4 Choose the Virtual Domain to which to move the interface.
- 5 Select OK.  
The physical interface moves to the virtual domain. Firewall IP pools and virtual IP added for this interface are deleted. You should manually delete any routes that include this interface.

#### To add VLAN subinterfaces to a virtual domain

A virtual domain must contain at least two interfaces. These can be physical interfaces or VLAN interfaces. VLAN subinterfaces are usually not in the same virtual domain as the physical interfaces that they are added to.

To add a new VLAN to a virtual domain in NAT/Route mode, see [“To add a VLAN subinterface in NAT/Route mode” on page 65](#). To add a new VLAN to a virtual domain in Transparent mode, see [“To add a VLAN subinterface in Transparent mode” on page 70](#).

The following procedure describes how to move a VLAN subinterface from one virtual domain to another. You cannot remove a VLAN subinterface from a virtual domain if firewall policies have been added for it. Delete the firewall policies or remove the VLAN subinterface from the firewall policies first. If the VLAN subinterface has been added to a zone, it is removed from the zone when you move it to a different virtual domain.

- 1 Go to **System > Network > Interface**.
- 2 Set Virtual domain to All or to the name of the virtual domain that currently contains the VLAN subinterface.
- 3 Select Edit for the VLAN subinterface you want to move.
- 4 Choose the Virtual Domain to which to move the VLAN subinterface.
- 5 Select OK.  
The VLAN subinterface moves to the virtual domain. Firewall IP pools and virtual IP added for this VLAN subinterface are deleted. You should manually delete any routes that include this VLAN subinterface.

#### To view the interfaces in a virtual domain

- 1 Go to **System > Network > Interface**.
- 2 Choose the Virtual domain you want to view.  
The interfaces added to this virtual domain are listed.

#### To add zones to a virtual domain

The following procedure applies to NAT/Route and Transparent mode.

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain to add zones to.

- 4 Select OK.
- 5 Go to **System > Network > Zone**.
- 6 Select Create new.  
See [“Zone” on page 58](#). Any zones that you add are added to the current virtual domain.

## Configuring routing for a virtual domain

### To configure routing for a virtual domain in NAT/Route mode

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure routing.
- 4 Select OK.
- 5 Go to **Router**.
- 6 Configure routing for the current virtual domain as required.  
See [“Router” on page 141](#). Network traffic entering this virtual domain is routed only by the routing configuration for the current virtual domain.

### To configure the routing table for a virtual domain in Transparent mode

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure routing.
- 4 Select OK.
- 5 Go to **System > Network > Routing Table**.
- 6 Configure the routing table for the current virtual domain as required.  
See [“Routing table \(Transparent Mode\)” on page 61](#). Network traffic entering this virtual domain is routed only by the static routes added to the current virtual domain.

## Configuring firewall policies for a virtual domain

### To add firewall policies to a virtual domain

The following procedure applies to NAT/Route and Transparent mode.

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select Change following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure firewall policies.
- 4 Select OK.
- 5 Go to **Firewall > Policy**.

- 6 Select **Create new** to add firewall policies to the current virtual domain. See [“Policy” on page 190](#). You can only add firewall policies for the physical interfaces, VLAN subinterfaces, or zones added to the current virtual domain. The firewall policies that you add are only visible when you are viewing the current virtual domain. Network traffic accepted by the interfaces and VLAN subinterfaces added to this virtual domain is controlled by the firewall policies added to this virtual domain

#### To add firewall addresses to a virtual domain

The following procedure applies to NAT/Route and Transparent mode.

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select **Change** following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure firewall addresses.
- 4 Select **OK**.
- 5 Go to **Firewall > Address**.
- 6 Add new firewall addresses, address ranges, and address groups to the current virtual domain. See [“Address” on page 198](#).

#### To add IP pools to a virtual domain

The following procedure applies to NAT/Route mode.

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select **Change** following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure firewall IP pools.
- 4 Select **OK**.
- 5 Go to **Firewall > IP Pool**.
- 6 Add new IP pools as required for the current virtual domain. See [“IP pool” on page 219](#).

#### To add Virtual IPs to a virtual domain

The following procedure applies to NAT/Route mode.

- 1 Go to **System > Virtual domain > Virtual domains**.
- 2 Select **Change** following the current virtual domain name above the table.
- 3 Choose the virtual domain for which to configure virtual IPs.
- 4 Select **OK**.
- 5 Go to **Firewall > Virtual IP**.
- 6 Add new virtual IPs as required for the current virtual domain. See [“Virtual IP” on page 214](#).

## Configuring IPSec VPN for a virtual domain

### To configure VPN for a virtual domain

The following procedure applies to NAT/Route and Transparent mode.

- 1** Go to **System > Virtual domain > Virtual domains**.
- 2** Select Change following the current virtual domain name above the table.
- 3** Choose the virtual domain for which to configure VPN.
- 4** Select OK.
- 5** Go to **VPN**.
- 6** Configure IPSec VPN, PPTP, L2TP, and certificates as required. See [“VPN” on page 245](#).

# Router

This chapter describes how to configure FortiGate routing and RIP. It contains the following sections:

- [Static](#)
- [Policy](#)
- [RIP](#)
- [Router objects](#)
- [Monitor](#)
- [CLI configuration](#)

## Static

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

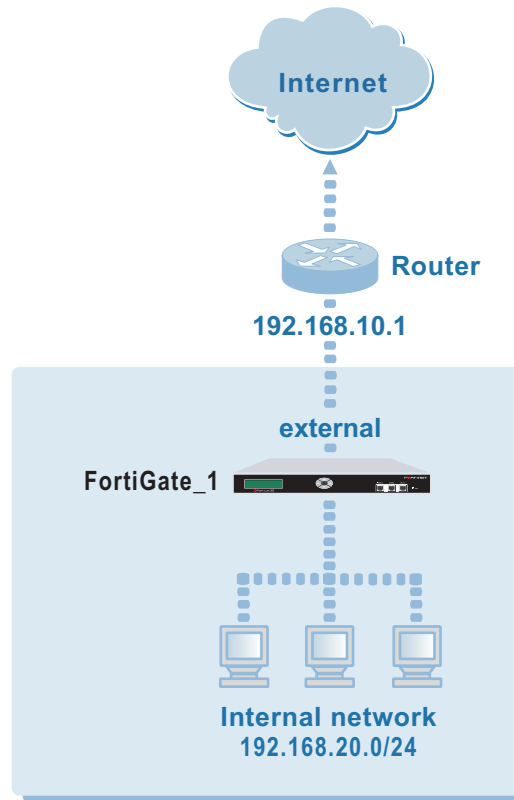
You configure routes by defining the destination IP address and netmask of packets that the FortiGate unit is intended to intercept, and specifying a (gateway) IP address for those packets. The gateway address specifies the next hop router to which traffic will be routed.

You can decrease the distance value of a static route to indicate that the route is preferable compared to another static route that specifies a different gateway to the same destination network. Routes having lower administrative distances are preferable and are selected first when two or more routes to the same destination network are available.

The FortiGate unit routes packets using a best match algorithm (the order of static routes in the list is ignored). To select a route for a packet, the FortiGate unit checks the destination address of the packet and searches through the routing table for the best matching destination address. If a match is found, the packet is forwarded to the specified gateway. If no match is found, the FortiGate unit routes the packet to the gateway specified in the default route. The value 0.0.0.0/0.0.0.0 (all destinations) is reserved for the default route. To route packets according to the default route, you must specify a gateway address and outbound interface for the default route.

For example, consider [Figure 50](#), which shows a FortiGate unit connected to a router. To ensure that all outbound packets destined to any network beyond the router are routed to the correct destination, you must edit the default configuration and make the router the default gateway for the FortiGate unit.

**Figure 50: Making a router the default gateway**



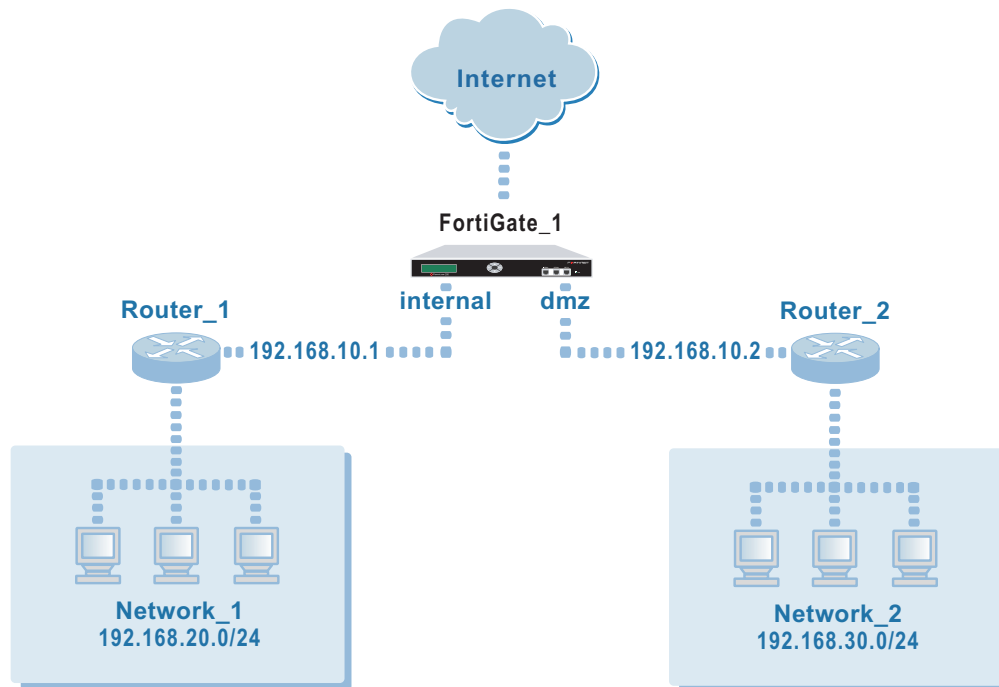
To route outbound packets from the internal network to destinations that are not on network 192.168.20.0/24, you would edit the default static route and include the following settings:

- Destination IP/mask: 0.0.0.0/0.0.0.0
- Gateway: 192.168.10.1
- Device: Name of the interface connected to network 192.168.10.0/24 (e.g. external).
- Distance: 10

The Gateway setting specifies the IP address of the next hop router interface to the FortiGate `external` interface. The interface behind the router (192.168.10.1) is the default gateway for FortiGate\_1.

In some cases, there may be routers behind the FortiGate unit. If the destination IP address of a packet is not on the local network but is on a network behind one of those routers, the FortiGate routing table must include a static route to that network. For example, in [Figure 51](#), the FortiGate unit must be configured with static routes to interfaces 192.168.10.1 and 192.168.10.2 in order to forward packets to Network\_1 and Network\_2 respectively.

Figure 51: Destinations on networks behind internal routers



To route packets from Network\_1 to Network\_2, Router\_1 must be configured to use the FortiGate `internal` interface as its default gateway. On the FortiGate unit, you would create a new static route with these settings:

Destination IP/mask: 192.168.30.0/24

Gateway: 192.168.10.2

Device: `dmz`

Distance: 10

To route packets from Network\_2 to Network\_1, Router\_2 must be configured to use the FortiGate `dmz` interface as its default gateway. On the FortiGate unit, you would create a new static route with these settings:

Destination IP/mask: 192.168.20.0/24

Gateway: 192.168.10.1

Device: `internal`

Distance: 10

## Static route list

Figure 52: Static routes

Create New						
#	IP	Mask	Gateway	Device	Distance	
1	0.0.0.0	0.0.0.0	192.168.100.1	external	10	
2	192.168.20.0	255.255.255.0	192.168.20.1	internal	10	

<b>Create New</b>	Add a new static route.
<b>#</b>	The sequence number for this route.
<b>IP</b>	The destination IP address for this route.
<b>Mask</b>	The netmask for this route.
<b>Gateway</b>	The IP address of the first next hop router to which this route directs traffic.
<b>Device</b>	The name of the FortiGate interface through which to route traffic.
<b>Distance</b>	The administrative distance for the route.
	The Delete, Edit, and Move to icons.

## Static route options

**Figure 53: Static route configuration**

<b>Destination IP/Mask</b>	Enter the destination IP address and netmask for this route. The value 0.0.0.0/0.0.0.0 is reserved for the default route.
<b>Gateway</b>	Enter the IP address of the first next hop router to which this route directs traffic.
<b>Device</b>	Select the name of the FortiGate interface through which to route traffic.
<b>Distance</b>	Enter the administrative distance for the route. Using administrative distance you can specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. Distance can be an integer from 1-255.

### To add or edit a static route

- 1 Go to **Router > Static > Static Route**.
- 2 Select Create New to add a new route or select the edit icon beside an existing route to edit that route.
- 3 Enter the Destination IP address and netmask for the route.
- 4 Add the Gateway IP address.
- 5 For Device, select the FortiGate interface through which to route traffic for this route.
- 6 If required, change the administrative Distance.
- 7 Select OK.

### To move static routes

- 1 Go to **Router > Static > Static Route**.
- 2 Select the Move to icon beside the route you want to move. Current Order shows the existing number for this route.



**Figure 54: Move a static route**

The screenshot shows a dialog box titled "Move Routing Policy". It contains a "Current Order" field with the value "2". Below it, there are two radio buttons: "Before" (which is selected) and "After". To the right of the "After" radio button is an empty text input field. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

- 3 For Move to, select either Before or After and type the number that you want to place this route before or after.

- 4 Select OK.

The route is displayed in the new location on the static route list.

## Policy





Using policy routing you can configure the FortiGate unit to route packets based on:

- Source address
- Protocol, service type, or port range
- Incoming or source interface

The FortiGate unit starts at the top of the policy routing list and attempts to match the packet with a policy. The policy route supplies the next hop gateway as well as the FortiGate interface to be used by the traffic. If no policy route matches the packet, the FortiGate unit routes the packet using the regular routing table.

### Policy route list

**Figure 55: Policy routes**

Create New					
#	Incoming	Outgoing	Source	Destination	
1	internal	external	192.168.10.0 / 255.255.255.0	100.100.100.0 / 255.255.255.0	 
2	internal	external	192.168.20.0 / 255.255.255.0	200.200.200.0 / 255.255.255.0	 

**Create New** Add a new policy route.

**#** The sequence number for this policy route.

**Incoming** The policy route attempts to match packets received on this interface.

**Outgoing** The policy route sends packets out this interface.

**Source** The policy route matches packets that have this source IP address and netmask.

**Destination** The policy route matches packets that have this destination IP address and netmask.

The Delete, and Edit icons.

## Policy route options

Figure 56: Policy route configuration

<b>Protocol</b>	Match packets that have this protocol number.
<b>Incoming Interface</b>	Match packets that are received on this interface.
<b>Source Address / Mask</b>	Match packets that have this source IP address and netmask.
<b>Destination Address / Mask</b>	Match packets that have this destination IP address and netmask.
<b>Destination Ports</b>	Match packets that have this destination port range. To match a single port, enter the same port number for both From and To.
<b>Outgoing Interface</b>	Send packets that match this policy route, out this interface.
<b>Gateway Address</b>	Send packets that match this policy route to this next hop router.

### To add a policy route

- 1 Go to **Router > Policy Route**.
- 2 Select Create New to add a new policy route or select the edit icon beside an existing policy route to edit that policy route.
- 3 Optionally enter a Protocol number.
- 4 Select the Incoming Interface.
- 5 Enter the Source Address / Mask and the Destination Address / Mask.
- 6 Optionally enter the Destination Ports.
- 7 Select the Outgoing Interface.
- 8 Enter the Gateway Address.
- 9 Select OK.

## RIP

The FortiGate implementation of the Routing Information Protocol (RIP) supports both RIP version 1 as defined by RFC 1058, and RIP version 2 as defined by RFC 2453. RIP version 2 enables RIP messages to carry more information, and to support simple authentication and subnet masks.

RIP is a distance-vector routing protocol intended for small, relatively homogeneous, networks. RIP uses hop count as its routing metric. Each network is usually counted as one hop. The network diameter is limited to 15 hops.

## General

Figure 57: RIP General settings

The screenshot shows the 'RIP General settings' configuration page. It includes the following elements:

- RIP Version:** Radio buttons for '1', '2', and 'Both'. '2' is selected.
- Default Metric:** Input field containing '1', with '(1-16)' indicating the valid range.
- Enable Default-information-originate:** An unchecked checkbox.
- RIP Timers:**
  - Update:** Input field containing '30', with '(seconds)' and '(1-255)'.
  - Garbage:** Input field containing '120', with '(seconds)' and '(1-255)'.
  - Timeout:** Input field containing '180', with '(seconds)' and '(1-255)'.
- Redistribute:**
  - Connected:** Unchecked checkbox.
    - Metric:** Input field containing '0', with '(1-16)'.
    - Route-map:** Dropdown menu.
  - Static:** Unchecked checkbox.
    - Metric:** Input field containing '0', with '(1-16)'.
    - Route-map:** Dropdown menu.
- Apply:** A button at the bottom center.

<b>RIP Version</b>	Enable sending and receiving RIP version 1 packets, RIP version 2 packets, or both for all RIP-enabled interfaces. You can override this setting on a per interface basis. See <a href="#">"Interface options"</a> on page 150.
<b>Default Metric</b>	For non-default routes in the static routing table and directly connected networks the default metric is the metric that the FortiGate unit advertises to adjacent routers. This metric is added to the metrics of learned routes. The default metric can be a number from 1 to 16.
<b>Enable Default-information-originate</b>	Advertise a default static route into RIP.
<b>RIP Timers:</b>	RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings.
<b>Update</b>	The time interval in seconds between RIP updates.
<b>Garbage</b>	The time in seconds that must elapse after the timeout interval for a route expires, before RIP deletes the route. If RIP receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable.
<b>Timeout</b>	The time interval in seconds after which a route is declared unreachable. The route is removed from the routing table. RIP holds the route until the garbage timer expires and then deletes the route. If RIP receives an update for the route before the timeout timer expires, then the timeout timer is restarted. If RIP receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. The value of the timeout timer should be at least three times the value of the update timer.
<b>Redistribute:</b>	Advertise routes learned from static routes, or a direct connection to the destination network.
<b>Connected</b>	Advertise routes learned from directly connected networks.
<b>Metric</b>	Enter the metric to be used for the redistributed connected routes.

<b>Route-map</b>	Enter the name of the route map to use for the redistributed connected routes. For information on how to configure route maps, see <a href="#">“Route-map list” on page 157</a> .
<b>Static</b>	Advertise routes learned from static routes.
<b>Metric</b>	Enter the metric to be used for the redistributed static routes.
<b>Route-map</b>	Enter the name of the route map to use for the redistributed static routes. For information on how to configure route maps, <a href="#">“Route-map list” on page 157</a> .

### To configure RIP general settings

- 1 Go to **Router > RIP > General**.
- 2 Select the default RIP Version.
- 3 Change the Default Metric if required.
- 4 Select Enable Default-information-originate if the configuration requires advertising a default static route into RIP.
- 5 Only change the RIP timers if required.  
RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings.
- 6 Select Apply.

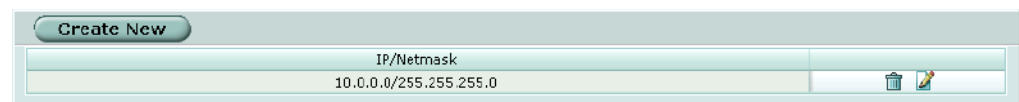
### To configure RIP route redistribution

- 1 Go to **Router > RIP > General**.
- 2 Select Connected or Static or both.
- 3 Enter the Default Metric to be used for the redistributed routes.
- 4 Select a Route-map name.
- 5 Select Apply.

## Networks list

Identify the networks for which to send and receive RIP updates. If a network is not specified, interfaces in that network will not be advertised in RIP updates.

**Figure 58: RIP Networks list**



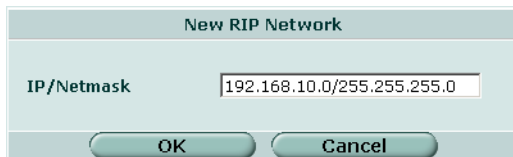
**Create New** Add a new RIP network.

**IP/Netmask** The IP address and netmask for the RIP network.

The Delete, and Edit icons.

## Networks options

Figure 59: RIP Networks configuration



### To configure a RIP network

- 1 Go to **Router > RIP > Networks**.
- 2 Select Create New to add a new RIP network or select the edit icon beside an existing RIP network to edit that RIP network.
- 3 Enter the IP address and netmask for the network.
- 4 Select OK.

## Interface list

Configure RIP version 2 authentication, RIP version send and receive for the specified interface, and configure and enable split horizon.

Authentication is only available for RIP version 2 packets sent and received by an interface. Set authentication to None if Send Version or Receive Version are set to 1 or 1 2.

Figure 60: RIP interface list

Create New					
Interface	Send Version	Receive Version	Split-Horizon	Authentication	
internal	2	2	Poisoned reverse	MD5	 

- Create New** Add a new RIP interface.
- Interface** The FortiGate interface name.
- Send Version** The RIP send version for this interface.
- Receive Version** The RIP receive version for this interface.
- Split-Horizon** The split horizon type.
- Authentication** The authentication type.
- The Delete and Edit icons.

## Interface options

Figure 61: RIP interface configuration

<b>Interface</b>	The FortiGate interface name.
<b>Send Version</b>	RIP routing messages are UDP packets that use port 520. Select 1 to configure RIP to send RIP version 1 messages from an interface. Select 2 to configure RIP to send RIP version 2 messages from an interface. Select Both to configure RIP to send both RIP version 1 and RIP version 2 messages from an interface. Setting the Send Version here overrides the default RIP version for this interface.
<b>Receive Version</b>	RIP routing messages are UDP packets that use port 520. Select 1 to configure RIP to listen for RIP version 1 messages on an interface. Select 2 to configure RIP to listen for RIP version 2 messages on an interface. Select Both to configure RIP to listen for both RIP version 1 and RIP version 2 messages on an interface. Setting the Receive Version here overrides the default RIP version for this interface.
<b>Split-Horizon</b>	Configure RIP to use either regular or poisoned reverse split horizon on this interface. Select Regular to prevent RIP from sending updates for a route back out the interface from which it received that route. Select Poisoned reverse to send updates with routes learned on an interface back out the same interface but with the routes marked as unreachable.
<b>Authentication</b>	Select the authentication used for RIP version 2 packets sent and received by this interface. If you select None, no authentication is used. If you select Text, the authentication key is sent as plain text. If you select MD5, the authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the update packet, not the confidentiality of the routing information in the packet. In text mode the key is sent in clear text over the network. Text mode is usually used only to prevent network problems that can occur if an unwanted or misconfigured router is mistakenly added to the network.

- Password** Enter a password (key) to use for authentication for RIP version 2 packets sent and received by this interface. Enter a password here when you only want to configure one key. The key can be up to 35 characters long.
- Key-chain** Enter the name of the key chain to use for authentication for RIP version 2 packets sent and received by this interface. Use key chains when you want to configure multiple keys. For information on how to configure key chains, see [“Key chain list” on page 160](#).

**To configure a RIP interface**

- 1 Go to **Router > RIP > Interface**.
- 2 Select the edit icon beside an Interface to configure that interface.
- 3 Select a Send Version if you want to override the default send version for this interface.
- 4 Select a Receive Version if you want to override the default receive version for this interface.
- 5 Select the Split-Horizon check box to enable split horizon.
- 6 Select either Regular or Poisoned reverse to set the split horizon type.
- 7 Select the Authentication mode.
- 8 Select Password and enter a password (key) if this interface is using RIP version 2 and if you are configuring only one key for this interface and do not want to use a key chain.
- 9 Select Key-chain and select the key chain to use if this interface is using RIP version 2 and you want to use key chains for authentication for this interface.
- 10 Select OK.

**Distribute list**

Use distribute lists to filter incoming or outgoing updates using an access list or a prefix list. If you do not specify an interface, the filter will be applied to all interfaces in the current virtual domain.



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

You must configure the access list or prefix list that you want the distribute list to use before you configure the distribute list. For more information on configuring access lists and prefix lists, see [“Access list” on page 154](#) and [“Prefix list” on page 155](#).

**Figure 62: RIP Distribute list**

Create New				
Direction	Filter	Interface	Enable	
In	prefix-list/pref_list1	internal		
Out	access-list/acc_list1			

<b>Create New</b>	Add a new distribute list.
<b>Direction</b>	The direction for the filter.
<b>Filter</b>	The type of filter and the filter name.
<b>Interface</b>	The interface to use this filter on. If no interface name is displayed, this distribute list is used for all interfaces.
<b>Enable</b>	The status of this distribute list. The Delete and Edit icons.

## Distribute list options

**Figure 63: RIP Distribute list configuration**

<b>Direction</b>	Set the direction for the filter. Select In to filter incoming packets. Select Out to filter outgoing packets.
<b>prefix-list</b>	Select prefix-list to use a prefix list for this distribute list. Select the name of the prefix list to use for this distribute list.
<b>access-list</b>	Select access-list to use an access list for this distribute list. Select the name of the access list to use for this distribute list.
<b>Interface</b>	Select the name of the interface to apply this distribute list to. If you do not specify an interface, this distribute list will be used for all interfaces.
<b>Enable</b>	Select Enable to enable the distribute list.

### To configure a distribute list

- 1 Go to **Router > RIP > Distribute List**.
- 2 Select Create New to add a new distribute list or select the edit icon beside an existing distribute list to edit that distribute list.
- 3 Set Direction to In or Out.
- 4 Select either prefix-list or access-list.
- 5 Select the prefix list or access list to use for this distribute list.
- 6 Select an interface to apply this distribute list to, or select the blank entry to apply this distribute list to all interfaces.
- 7 Select or clear the Enable check box to enable or disable this distribute list.
- 8 Select OK.







## Offset list

Use offset lists to add the specified offset to the metric of a route.



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

**Figure 64: RIP Offset list**

Create New					
Direction	Access-list	Offset	Interface	Enable	
Out	acc_list1	3	internal	<input checked="" type="checkbox"/>	 
In	acc_list2	2	internal	<input checked="" type="checkbox"/>	 

- Create New** Add a new offset list.
- Direction** The direction for the offset list.
- Access-list** The access list to use for this offset list.
- Offset** The offset number to add to the metric for this offset list.
- Interface** The interface to match for this offset list.
- Enable** The status of this offset list.  
The Delete and Edit icons.

## Offset list options

**Figure 65: RIP Offset list configuration**

**New RIP Offset-list**

Direction ▼

Access-list ▼

Offset  (1-16)

Interface ▼

Enable

- Direction** Select In to apply the offset to the metrics of incoming routes. Select out to apply the offset to the metrics of outgoing routes.
- Access-list** Select the access list to use for this offset list. The access list is used to determine which routes to add the metric to.
- Offset** Enter the offset number to add to the metric. Enter a number from 1 to 16.
- Interface** Select the interface to match for this offset list.
- Enable** Select Enable to enable this offset list.

### To configure an offset list

- 1 Go to **Router > RIP > Offset List**.
- 2 Select Create New to add a new offset list or select the edit icon beside an existing offset list to edit that offset list.

- 3 Set Direction to In or Out.
- 4 Enter the offset number.
- 5 Select the interface to match for this offset list.
- 6 Check or clear the Enable check box to enable or disable this offset list.
- 7 Select OK.

## Router objects

Router objects are a set of tools used by routing protocols and features.

### Access list

Access lists are filters used by FortiGate routing features.

Each rule in an access list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and whether to match the prefix exactly or to match the prefix and any more specific prefix.

The FortiGate unit attempts to match a packet against the rules in an access list starting at the top of the list. If it finds a match for the prefix it takes the action specified for that prefix. If no match is found the default action is deny.

For an access list to take effect it must be called by another FortiGate routing feature such as RIP or OSPF.

**Figure 66: Access list**

Create New			
Name	Action	Prefix	
▼ acc_list1			🗑️ ➕
1	Deny	192.168.50.0/255.255.255.0	🗑️ ✎
2	Permit	192.168.0.0/255.255.0.0	🗑️ ✎
▶ acc_list2			🗑️ ➕

- Create New** Add a new access list name. An access list and a prefix list cannot have the same name.
  - Name** The access list name.
  - Action** The action to take for the prefix in an access list entry.
  - Prefix** The prefix in an access list entry.
- The Delete, Add access-list entry, and Edit icons.

### New access list

**Figure 67: Access list name configuration**

New RIP Access-list

Access-list

### To add an access list name

- 1 Go to **Router > Router Objects > Access List**.
- 2 Select Create New.
- 3 Enter a name for the access list.
- 4 Select OK.

## New access list entry

Figure 68: Access list entry configuration

<b>list Entry</b>	The access list name and the number of this entry.
<b>Action</b>	Set the action to take for this prefix to Permit or Deny.
<b>Prefix</b>	Select Match any to match any prefix. Select Match a network address and enter the prefix (IP address and netmask) for this access list rule.
<b>Exact match</b>	By default, access list rules are matched on the prefix or any more specific prefix. Enable Exact match to match only the configured prefix.

### To configure an access list entry

- 1 Go to **Router > Router Objects > Access List**.
- 2 Select the Add access-list entry icon to add a new access list entry or select the edit icon beside an existing access list entry to edit that entry.
- 3 Select Permit or Deny for the Action to take for the prefix in this access list entry.
- 4 Select either Match any or Match a network address.
- 5 If you selected Match a network address, enter the IP address and netmask that define the prefix for this access list entry.
- 6 Select Exact match if required.
- 7 Select OK.

## Prefix list

A prefix list is an enhanced version of an access list that allows you to control the length of the prefix netmask.

Each rule in a prefix list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and maximum and minimum prefix length settings.

The FortiGate unit attempts to match a packet against the rules in a prefix list starting at the top of the list. If it finds a match for the prefix, it takes the action specified for that prefix. If no match is found the default action is deny.

For a prefix list to take effect it must be called by another FortiGate routing feature such as RIP or OSPF.

**Figure 69: Prefix list**

Name	Action	Prefix	GE	LE	
▼ prf_list1					🗑️ ➕
1	Permit	192.168.100.0/255.255.255.0	26	30	🗑️ ✎
2	Deny	10.1.0.0/255.255.0.0	20	25	🗑️ ✎
3	Deny	Any			🗑️ ✎
▶ prf_list2					🗑️ ➕

- Create New** Add a new prefix list name. An access list and a prefix list cannot have the same name.
- Name** The prefix list name.
- Action** The action to take for the prefix in a prefix list entry.
- Prefix** The prefix in a prefix list entry.
- GE** The greater than or equal to number.
- LE** The less than or equal to number.
- The Delete, Add prefix-list entry, and Edit icons.

## New Prefix list

**Figure 70: Prefix list name configuration**

### To add a prefix list name

- 1 Go to **Router > Router Objects > Prefix List**.
- 2 Select Create New.
- 3 Enter a name for the prefix list.
- 4 Select OK.

## New prefix list entry

Figure 71: Prefix list entry configuration

The screenshot shows a configuration window titled "New Prefix-list Entry". It contains the following fields and options:

- list Entry:** perf\_list1 -> #1
- Action:** A dropdown menu set to "Permit".
- Prefix:** Radio buttons for "Match any" (unselected) and "Match a network address" (selected).
- Match a network address:** A text input field containing "192.168.100.0/24".
- Greater or equal to:** A checked checkbox with a text input field containing "26" and "(0 -32)" to its right.
- Less or equal to:** A checked checkbox with a text input field containing "30" and "(0 -32)" to its right.
- Buttons:** "OK" and "Cancel" buttons at the bottom.

<b>list Entry</b>	The prefix list name and the number of this entry.
<b>Action</b>	Set the action to take for this prefix to Permit or Deny.
<b>Prefix</b>	Select Match any to match any prefix. Select Match a network address and enter the prefix (IP address and netmask) for this prefix list entry. The length of the netmask should be less than the setting for Greater or equal to.
<b>Greater or equal to</b>	Match prefix lengths that are greater than or equal to this number. The setting for Greater or equal to should be less than the setting for Less or equal to. The setting for Greater or equal to should be greater than the netmask set for Prefix. The number can be from 0 to 32.
<b>Less or equal to</b>	Match prefix lengths that are less than or equal to this number. The setting for Less or equal to should be greater than the setting for Greater or equal to. The number can be from 0 to 32.

### To configure a prefix list entry

- 1 Go to **Router > Router Objects > Prefix List**.
- 2 Select the Add prefix-list entry icon to add a new prefix list entry or select the edit icon beside an existing prefix list entry to edit that entry.
- 3 Select Permit or Deny for the Action to take for the prefix in this prefix list entry.
- 4 Select either Match any or Match a network address.
- 5 If you selected Match a network address, enter the IP address and netmask that define the prefix for this prefix list entry.
- 6 Select Greater or equal to and enter a number from 0 to 32 to match prefix lengths that are greater than or equal to this number.
- 7 Select Less or equal to and enter a number from 0 to 32 to match prefix lengths that are less than or equal to this number.
- 8 Select OK.

## Route-map list

Route maps are a specialized form of filter. Route maps are similar to access lists, but have enhanced matching criteria, and in addition to permit or deny actions can be configured to make changes as defined by set statements.

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

For a route map to take effect it must be called by another FortiGate routing feature such as RIP.

**Figure 72: Route map list**

Create New			
Name	Action	Route-map rules	
▼ rtmp2			🗑️ ➕
1	Deny	match: address=access-list/acc_list2 set:	🗑️ ✎
2	Permit	match: metric=2 set: metric=4	🗑️ ✎

- Create New** Add a new route map name.
- Name** The route map name.
- Action** The action to take for this entry in the route map.
- Route-map rules** The rules for a route map entry.  
The Delete, Add route-map entry, and Edit icons.

## New Route-map

**Figure 73: Route map name configuration**

### To add a route map name

- 1 Go to **Router > Router Objects > Route-map**.
- 2 Select Create New.
- 3 Enter a name for the route map.
- 4 Select OK.

## Route-map list entry

Figure 74: Route map entry configuration

<b>Route-map entry</b>	The route map name and the ID number of this route map entry.
<b>Action</b>	Select Permit to permit routes that match this entry. Select Deny to deny routes that match this entry.
<b>Match:</b>	The criteria to match.
<b>Interface</b>	Match a route with the selected destination interface.
<b>Address</b>	Match a route if the destination address is included in the selected access list or prefix list.
<b>Next-hop</b>	Match a route that has a next hop router address included in the selected access list or prefix list.
<b>Metric</b>	Match a route with the specified metric. The metric can be a number from 1 to 16.
<b>Route Type</b>	Match a route that has the external type set to 1 or 2.
<b>Tag</b>	Match a route that has the specified tag.
<b>Set:</b>	The set criteria.
<b>Next-hop</b>	Set the next hop router address for a matched route.
<b>Metric</b>	Set a metric value of 1 to 16 for a matched route.
<b>Metric Type</b>	Set a metric value of 1 to 16 for a matched route.
<b>Tag</b>	Set a tag value for a matched route.

### To configure a route map entry

- 1 Go to **Router > Router Objects > Route Map**.
- 2 Select the Add route-map entry icon to add a new route map entry or select the edit icon beside an existing route map entry to edit that entry.
- 3 Select Permit or Deny for the Action to take for this route map entry.

- 4 Under Match, select the criteria to match.
- 5 Under Set, select the criteria to change.
- 6 Select OK.

### Key chain list

RIP version 2 uses authentication keys to ensure that the routing information exchanged between routers is reliable. For authentication to work both the sending and receiving routers must be set to use authentication, and must be configured with the same keys.

A key chain is a list of one or more keys and the send and receive lifetimes for each key. Keys are used for authenticating routing packets only during the specified lifetimes. The FortiGate unit migrates from one key to the next according to the scheduled send and receive lifetimes. The sending and receiving routers should have their system dates and times synchronized, but overlapping the key lifetimes ensures that a key is always available even if there is some difference in the system times. See [“System time” on page 81](#) for information on setting the FortiGate system date and time.

Figure 75: Key chain list

Key-chain	Accept Lifetime		Send Lifetime		
	Start	End	Start	End	
test1					
1	10:0:0 6/1/2004	Duration: 46800	10:0:0 6/1/2004	Duration: 46800	🗑️ ✎️
2	22:0:0 6/1/2004	Duration: 46800	22:0:0 6/1/2004	Duration: 46800	🗑️ ✎️
3	10:0:0 6/2/2004	Infinite	10:0:0 6/2/2004	Infinite	🗑️ ✎️

- Create New** Add a new key chain.
- Key-chain** The key chain name.
- Accept Lifetime** The time period in which to accept a key.
- Send Lifetime** The time period in which to send a key.
- Start End** The start and end times for the accept and send lifetimes.
- The Delete, Add key-chain entry, and Edit icons.

### New key chain

Figure 76: Key chain name configuration

**New Key-chain**

Key-chain name

#### To add a key chain name

- 1 Go to **Router > Router Objects > Key-chain**.
- 2 Select Create New.



- 3 Enter a name for the key chain.
- 4 Select OK.

## Key chain list entry

Figure 77: Key chain entry configuration

- Key-chain entry** The key chain name and the ID number for this key chain entry.
- Key** The key (password) can be up to 35 characters long.
- Accept Lifetime** Set the time period during which the key can be received.
- Send Lifetime** Set the time period during which the key can be sent.
- Start** For both accept and send lifetimes, set the start time and date for this entry in the key chain.
- End** For both accept and send lifetimes, set the end time. The end time can be a specified date and time, a duration in seconds (1 to 2147483646), or infinite for a key that never expires.

### To configure a key chain entry

- 1 Go to **Router > Router Objects > Key-chain**.
- 2 Select the Add key-chain entry icon to add a new key chain entry or select the Edit icon beside an existing key chain entry to edit that entry.
- 3 Enter a key.
- 4 Under Accept Lifetime, select the required hour, minute, second, year, month and day to start using this key for received routing updates.

- 5 Under Accept Lifetime, select Infinite, Duration or End time.
  - If you selected Duration, enter the time in seconds that this key should be active.
  - If you selected End time, select the required hour, minute, second, year, month and day to stop using this key for received routing updates.
- 6 Under Send Lifetime, select the required hour, minute, second, year, month and day to start using this key for sending routing updates.
- 7 Under Send Lifetime, select Infinite, Duration or End time.
  - If you selected Duration, enter the time in seconds that this key should be active.
  - If you selected End time, select the required hour, minute, second, year, month and day to stop using this key for sending routing updates.
- 8 Select OK.

## Monitor

Display the FortiGate routing table.

### Routing monitor list

Figure 78: Routing monitor

Type	Subtype	Network	Distance	Metric	Gateway	Interface	Up Time
Connected		10.0.0.0/24	0	0	0.0.0.0	dmz	
Connected		172.20.120.0/24	0	0	0.0.0.0	external	

<b>Type:</b>	Filter the display to show routes of the selected type.
<b>Network:</b>	Filter the display to show routes for the specified network.
<b>Gateway:</b>	Filter the display to show routes using the specified gateway.
<b>Apply Filter</b>	Filter the routes according to the criteria you have specified.
<b>Type</b>	The type of route. Type refers to how the FortiGate unit learned the route.
<b>Subtype</b>	The subtype for the route.
<b>Network</b>	The network for the route.
<b>Distance</b>	The administrative distance of the route.
<b>Metric</b>	The metric for the route.
<b>Gateway</b>	The gateway used by the route.
<b>Interface</b>	The interface used by the route.
<b>Up Time</b>	How long the route has been available.

#### To filter the routing monitor display

- 1 Go to **Router > Monitor > Routing Monitor**.
- 2 Select a type of route to display or select all to display routes of all types.  
For example, select Connected to display all the directly connected routes, or select RIP to display all the routes learned from RIP.

- 3 Specify the network for which to display routes.
- 4 Specify a gateway to display the routes using that gateway.
- 5 Select Apply Filter.



**Note:** You can configure Type, Network, and Gateway filters individually or in any combination.

## CLI configuration

This guide only covers Command Line Interface (CLI) commands, keywords, or variables (in bold) that are not represented in the web-based manager. For complete descriptions and examples of how to use CLI commands see the *FortiGate CLI Reference Guide*.

### get router info ospf

Use this command to display information about OSPF.

#### Command syntax

```
get router info ospf <keyword>
```

#### router info ospf command keywords and variables

Keywords and variables	Description	Availability
border-routers	Show OSPF routing table entries that have an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) as a destination.	All models.
database	Show the entries in the OSPF routing database.	All models.
interface	Show the status of the FortiGate interfaces and whether OSPF is enabled for each interface.	All models.
neighbor	Show information about OSPF neighbors.	All models.
route	Show the OSPF routing table.	All models.
status	Show the status of the OSPF process.	All models.
virtual-links	Show information about OSPF virtual links.	All models.

#### Examples

```
get router info ospf database
get router info ospf interface
```

### get router info protocols

Show the current state of active routing protocols.

#### Command syntax

```
get router info protocols
```

## get router info rip

Use this command to display information about RIP.

### Command syntax

```
get router info rip <keyword>
```

### router info rip command keywords and variables

Keywords and variables	Description	Availability
database	Show the entries in the RIP routing database.	All models.
interface	Show the status of the FortiGate interfaces and whether RIP is enabled for each interface.	All models.

### Examples

```
get router info rip database
get router info rip interface
```

## config router ospf

Use this command to configure open shortest path first (OSPF) on the FortiGate unit.

OSPF is an open protocol based on the shortest path first algorithm. OSPF is a link state protocol capable of routing larger networks than the simpler distance vector RIP protocol. An OSPF autonomous system (AS) or routing domain is a group of areas connected to a backbone area. A router connected to more than one area is an area border router (ABR). Routing information is contained in a link state database. Routing information is communicated between routers using link state advertisements (LSAs). More information on OSPF can be found in RFC 2328.

### Command syntax pattern

```
config router ospf
    set <keyword> <variable>
end

config router ospf
    unset <keyword>
end

get router ospf

show router ospf
```

The `config router ospf` command has 7 subcommands.

```
config area
config distribute-list
config neighbor
config network
config ospf-interface
config redistribute
```

## config summary-address



**Note:** In the following table, only the `router-id` keyword is required. All other keywords are optional.

## ospf command keywords and variables

Keywords and variables	Description	Default	Availability
<code>abr-type {cisco   ibm   shortcut   standard}</code>	Specify the behavior of a FortiGate unit acting as an OSPF area border router (ABR) when it has multiple attached areas and has no backbone connection. Selecting the ABR type compatible with the routers on your network can reduce or eliminate the need for configuring and maintaining virtual links. For more information, see RFC 3509.	cisco	All models.
<code>database-overflow {disable   enable}</code>	Enable or disable dynamically limiting link state database size under overflow conditions. Enable this command for FortiGate units on a network with routers that because of limited resources may not be able to maintain a complete link state database.	disable	All models.
<code>database-overflow-max-lsas &lt;lsas_integer&gt;</code>	If you have enabled <code>database-overflow</code> , set the limit for the number of external link state advertisements (LSAs) that the FortiGate unit can keep in its link state database before entering the overflow state. The <code>lsas_integer</code> must be the same on all routers attached to the OSPF area and the OSPF backbone. The valid range for <code>lsas_integer</code> is 0 to 4294967294.	10000	All models.
<code>database-overflow-time-to-recover &lt;seconds_integer&gt;</code>	Enter the time, in seconds, after which the FortiGate unit will attempt to leave the overflow state. If <code>seconds_integer</code> is set to 0, the FortiGate unit will not leave the overflow state until restarted. The valid range for <code>seconds_integer</code> is 0 to 65535.	300	All models.
<code>default-information-metric &lt;metric_integer&gt;</code>	Specify the metric for the default route set by the <code>default-information-originate</code> command. The valid range for <code>metric_integer</code> is 1 to 16777214.	10	All models.
<code>default-information-metric-type {1   2}</code>	Specify the OSPF external metric type for the default route set by the <code>default-information-originate</code> command.	2	All models.
<code>default-information-originate {always   disable   enable}</code>	Enter <code>enable</code> to advertise a default route into an OSPF routing domain. Use <code>always</code> to advertise a default route even if the FortiGate unit does not have a default route in its routing table.	disable	All models.
<code>default-information-route-map &lt;name_str&gt;</code>	If you have set <code>default-information-originate</code> to <code>always</code> , and there is no default route in the routing table, you can configure a route map to define the parameters that OSPF uses to advertise the default route.	No default.	All models.

**ospf command keywords and variables (Continued)**

Keywords and variables	Description	Default	Availability
default-metric <metric_integer>	Specify the default metric that OSPF should use for redistributed routes. The valid range for <code>metric_integer</code> is 1 to 16777214.	10	All models.
distance <distance_integer>	Configure the administrative distance for all OSPF routes. Using administrative distance you can specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. The valid range for <code>distance_integer</code> is 1 to 255.	110	All models.
passive-interface <name_str>	OSPF routing information is not sent or received through the specified interface.	No default.	All models.
rfc1583-compatible {disable   enable}	Enable or disable RFC 1583 compatibility. RFC 1583 compatibility should be enabled only when there is another OSPF router in the network that only supports RFC 1583. When RFC 1583 compatibility is enabled, routers choose the path with the lowest cost. Otherwise, routers choose the lowest cost intra-area path through a non-backbone area.	disable	All models.
router-id <address_ipv4>	Set the router ID. The router ID is a unique number, in IP address dotted decimal format, that is used to identify an OSPF router to other OSPF routers. The router ID should not be changed while OSPF is running. A router ID of 0.0.0.0 is not allowed.	No default.	All models.
spf-timers <delay_integer> <hold_integer>	Change the default shortest path first (SPF) calculation delay time and frequency. The <code>delay_integer</code> is the time, in seconds, between when OSPF receives information that will require an SPF calculation and when it starts an SPF calculation. The valid range for <code>delay_integer</code> is 0 to 4294967295. The <code>hold_integer</code> is the minimum time, in seconds, between consecutive SPF calculations. The valid range for <code>hold_integer</code> is 0 to 4294967295. OSPF updates routes more quickly if the SPF timers are set low; however, this uses more CPU. A setting of 0 for <code>spf-timers</code> can quickly use up all available CPU.	5 10	All models.

**Example**

This example shows how to set the OSPF router ID to 1.1.1.1:

```
config router ospf
    set router-id 1.1.1.1
end
```

This example shows how to display the OSPF settings.

```
get router ospf
```

This example shows how to display the OSPF configuration.

```
show router ospf
```

## config area

Access the `config area` subcommand using the `config router ospf` command. Use this command to set OSPF area related parameters.

Routers in an OSPF autonomous system (AS) or routing domain are organized into logical groupings called areas. Areas are linked together by area border routers (ABRs). There must be a backbone area that all areas can connect to. You can use a virtual link to connect areas that do not have a physical connection to the backbone. Routers within an OSPF area maintain link state databases for their own areas.

## config area command syntax pattern



**Note:** Any IP address is a valid area ID. An area ID of 0.0.0.0 indicates the backbone area.

```
config area
  edit <id_ipv4>
    set <keyword> <variable>
  end

config area
  edit <id_ipv4>
    unset <keyword> <variable>
  end

config area
  delete <id_ipv4>
  end

config area
  edit <id_ipv4>
  get
  end

config area
  edit <id_ipv4>
  show
  end
```

The `config area` command has 3 subcommands.

```
config filter-list
config range
config virtual-link
```



**Note:** All area keywords are optional.

## area command keywords and variables

Keywords and variables	Description	Default	Availability
authentication {md5   none   text}	<p>Set the authentication type.</p> <p>Use the <code>authentication</code> keyword to define the authentication used for OSPF packets sent and received in this area. If you select <code>none</code>, no authentication is used. If you select <code>text</code>, the authentication key is sent as plain text. If you select <code>md5</code>, an authentication key is used to generate an MD5 hash.</p> <p>Both text mode and MD5 mode only guarantee the authenticity of the OSPF packet, not the confidentiality of the information in the packet.</p> <p>In text mode the key is sent in clear text over the network. Text mode is usually used only to prevent network problems that can occur if an unwanted or misconfigured router is mistakenly added to the area.</p> <p>If you configure authentication for interfaces, the authentication configured for the area is not used. Authentication passwords or keys are defined per interface. See "<a href="#">config ospf-interface</a>" on page 180.</p>	none	All models.
default-cost <cost_integer>	<p>Enter the metric to use for the summary default route in a stub area or not so stubby area (NSSA). A lower default cost indicates a more preferred route.</p> <p>The valid range for <code>cost_integer</code> is 1 to 16777214.</p>	10	All models.
nssa-default-information-originate {disable   enable}	<p>Enter <code>enable</code> to advertise a default route in a not so stubby area. Affects NSSA ABRs or NSSA Autonomous System Boundary Routers only.</p>	disable	All models.
nssa-default-information-originate-metric <metric_integer>	<p>Specify the metric for the default route set by the <code>nssa-default-information-originate</code> keyword.</p>	10	All models.
nssa-default-information-originate-metric-type {1   2}	<p>Specify the OSPF external metric type for the default route set by the <code>nssa-default-information-originate</code> keyword.</p>	2	All models.
nssa-redistribution {disable   enable}	<p>Enable or disable redistributing routes into a NSSA area.</p>	enable	All models.



**area command keywords and variables (Continued)**

Keywords and variables	Description	Default	Availability
nssa-translator-role {always   candidate   never}	A NSSA border router can translate the Type 7 LSAs used for external route information within the NSSA to Type 5 LSAs used for distributing external route information to other parts of the OSPF routing domain. Usually a NSSA will have only one NSSA border router acting as a translator for the NSSA. You can set the translator role to <code>always</code> to ensure this FortiGate unit always acts as a translator if it is in a NSSA, even if other routers in the NSSA are also acting as translators. You can set the translator role to <code>candidate</code> to have this FortiGate unit participate in the process for electing a translator for a NSSA. You can set the translator role to <code>never</code> to ensure this FortiGate unit never acts as the translator if it is in a NSSA.	candidate	All models.
shortcut {default   disable   enable}	Use this command to specify area shortcut parameters.	disable	All models.
stub-type {no-summary   summary}	Enter <code>no-summary</code> to prevent an ABR sending summary LSAs into a stub area. Enter <code>summary</code> to allow an ABR to send summary LSAs into a stub area.	summary	All models.
type {nssa   regular   stub}	Set the area type: <ul style="list-style-type: none"> <li>• Select <code>nssa</code> for a not so stubby area.</li> <li>• Select <code>regular</code> for a normal OSPF area.</li> <li>• Select <code>stub</code> for a stub area.</li> </ul>	regular	All models.

**Example**

This example shows how to configure a stub area with the id 15.1.1.1, a stub type of `summary`, a default cost of 20, and MD5 authentication.

```

config router ospf
  config area
    edit 15.1.1.1
      set type stub
      set stub-type summary
      set default-cost 20
      set authentication md5
    end
  end

```

This example shows how to display the settings for area 15.1.1.1.

```

config router ospf
  config area
    edit 15.1.1.1
      get
    end

```

This example shows how to display the configuration for area 15.1.1.1.

```
config router ospf
    config area
        edit 15.1.1.1
    show
end
```

## config filter-list

Access the `config filter-list` subcommand using the `config area` subcommand.

Use filter lists to control the import and export of LSAs into and out of an area. You can use access or prefix lists for OSPF area filter lists. For more information, see [“Access list” on page 154](#) and [“Prefix list” on page 155](#).

## config filter-list command syntax pattern

```
config filter-list
    edit <id_integer>
        set <keyword> <variable>
    end

config filter-list
    edit <id_integer>
        unset <keyword>
    end

config filter-list
    delete <id_integer>
    end

config filter-list
    edit <id_integer>
        get
    end

config filter-list
    edit <id_integer>
        show
    end
```



**Note:** Both keywords are required.

## filter-list command keywords and variables

Keywords and variables	Description	Default	Availability
direction {in   out}	Set the direction for the filter. Enter <code>in</code> to filter incoming packets. Enter <code>out</code> to filter outgoing packets.	out	All models.
list <name_str>	Enter the name of the access list or prefix list to use for this filter list.	No default.	All models.

## Example

This example shows how to use an access list named `acc_list1` to filter packets entering area 15.1.1.1.

```
config router ospf
    config area
        edit 15.1.1.1
            config filter-list
                edit 1
                    set direction in
                    set list acc_list1
            end
        end
    end
```

This example shows how to display the settings for area 15.1.1.1.

```
config router ospf
    config area
        edit 15.1.1.1
            get
        end
```

This example shows how to display the configuration for area 15.1.1.1.

```
config router ospf
    config area
        edit 15.1.1.1
            show
        end
```

## config range

Access the `config range` subcommand using the `config area` command.

Use the `area range` command to summarize routes at an area boundary. If the network numbers in an area are contiguous, the ABR advertises a summary route that includes all the networks within the area that are within the specified range.

## config range command syntax pattern

The range `id_integer` can be 0 to 4294967295.

```
config range
    edit <id_integer>
        set <keyword> <variable>
    end

config range
    edit <id_integer>
        unset <keyword>
    end

config range
    delete <id_integer>
end
```

```

config range
  edit <id_integer>
    get
  end

config range
  edit <id_integer>
    show
  end

```



**Note:** Only the `prefix` keyword is required. All other keywords are optional.

### range command keywords and variables

Keywords and variables	Description	Default	Availability
<code>advertise</code> { <code>disable</code>   <code>enable</code> }	Enable or disable advertising the specified range.	<code>enable</code>	All models.
<code>prefix</code> < <code>address_ipv4mask</code> >	Specify the range of addresses to summarize.	No default	All models.
<code>substitute</code> < <code>address_ipv4mask</code> >	Enter a prefix to advertise instead of the prefix defined for the range. The prefix 0.0.0.0 0.0.0.0 is not allowed.	No default.	All models.
<code>substitute-status</code> { <code>disable</code>   <code>enable</code> }	Enable or disable using a substitute prefix.	<code>disable</code>	All models.

### Example

This example shows how to set the prefix for range 1 of area 15.1.1.1.

```

config router ospf
  config area
    edit 15.1.1.1
      config range
        edit 1
          set prefix 1.1.0.0 255.255.0.0
        end
      end
    end
  end
end

```

This example shows how to display the settings for area 15.1.1.1.

```

config router ospf
  config area
    edit 15.1.1.1
      get
    end
  end
end

```

This example shows how to display the configuration for area 15.1.1.1.

```
config router ospf
    config area
        edit 15.1.1.1
    show
end
```

### config virtual-link

Access the `config virtual-link` subcommand using the `config area` command.

Use virtual links to connect an area to the backbone when the area has no direct connection to the backbone. A virtual link allows traffic from the area to transit a directly connected area to reach the backbone. The transit area cannot be a stub area. Virtual links can only be set up between two area border routers (ABRs).

### config virtual link command syntax pattern

```
config virtual-link
    edit <name_str>
        set <keyword> <variable>
    end

config virtual-link
    edit <name_str>
        unset <keyword>
    end

config virtual-link
    delete <name_str>
end

config virtual-link
    edit <name_str>
        get
    end

config virtual-link
    edit <name_str>
        show
    end
```



**Note:** Only the `peer` keyword is required. All other keywords are optional.

## virtual-link command keywords and variables

Keywords and variables	Description	Default	Availability
authentication {md5   none   text}	Set the authentication type. Use the <code>authentication</code> keyword to define the authentication used for OSPF packets sent and received over this virtual link. If you select <code>none</code> , no authentication is used. If you select <code>text</code> , the authentication key is sent as plain text. If you select <code>md5</code> , an authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the OSPF packet, not the confidentiality of the information in the packet. In text mode the key is sent in clear text over the network. Text mode is usually used only to prevent network problems that can occur if an unwanted or misconfigured router is mistakenly added to the area.	none	All models.
authentication-key <password_str>	Enter the password to use for <code>text</code> authentication. The <code>authentication-key</code> must be the same on both ends of the virtual link. The maximum length for the <code>authentication-key</code> is 15 characters.	No default.	All models. <code>authentication</code> must be set to <code>text</code> .
dead-interval <seconds_integer>	The time, in seconds, to wait for a hello packet before declaring a router down. The value of the <code>dead-interval</code> should be four times the value of the <code>hello-interval</code> . Both ends of the virtual link must use the same value for <code>dead-interval</code> . The valid range for <code>seconds_integer</code> is 1 to 65535.	40	All models.
hello-interval <seconds_integer>	The time, in seconds, between hello packets. Both ends of the virtual link must use the same value for <code>hello-interval</code> . The valid range for <code>seconds_integer</code> is 1 to 65535.	10	All models.
md5-key <id_integer><key_str>	Enter the key ID and password to use for MD5 authentication. Both ends of the virtual link must use the same key ID and key. The valid range for <code>id_integer</code> is 1 to 255. <code>key_str</code> is an alphanumeric string of up to 16 characters.	No default.	All models. <code>authentication</code> must be set to <code>md5</code> .
peer <address_ipv4>	The router id of the remote ABR. 0.0.0.0 is not allowed.	No default.	All models.

**virtual-link command keywords and variables (Continued)**

Keywords and variables	Description	Default	Availability
retransmit-interval <seconds_integer>	The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for seconds_integer is 1 to 65535.	5	All models.
transmit-delay <seconds_integer>	The estimated time, in seconds, required to send a link state update packet on this virtual link. OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the virtual link. Increase the value for transmit-delay on low speed links. The valid range for seconds_integer is 1 to 65535.	1	All models.

**Example**

This example shows how to configure a virtual link.

```

config router ospf
    config area
        edit 15.1.1.1
            config virtual-link
                edit vlnk1
                    set peer 1.1.1.1
            end
        end
    end

```

This example shows how to display the settings for area 15.1.1.1.

```

config router ospf
    config area
        edit 15.1.1.1
            get
        end
    end

```

This example shows how to display the configuration for area 15.1.1.1.

```

config router ospf
    config area
        edit 15.1.1.1
            show
        end
    end

```

**config distribute-list**

Access the `config distribute-list` subcommand using the `config router ospf` command.

Use this command to use an access list to filter the networks in routing updates. Routes not matched by any of the distribute lists will not be advertised.

You must configure the access list that you want the distribute list to use before you configure the distribute list. For more information on configuring access lists, see [“Access list” on page 154](#).

### config distribute-list command syntax pattern

```

config distribute-list
  edit <id_integer>
    set <keyword> <variable>
  end

config distribute-list
  edit <id_integer>
    unset <keyword>
  end

config distribute-list
  delete <id_integer>
  end

config distribute-list
  edit <id_integer>
    get
  end

config distribute-list
  edit <id_integer>
    show
  end

```



**Note:** Both keywords are required.

### distribute-list command keywords and variables

Keywords and variables	Description	Default	Availability
access-list <name_str>	Enter the name of the access list to use for this distribute list.	No default.	All models.
protocol {connected   rip   static}	Advertise only the routes discovered by the specified protocol and that are permitted by the named access list.	connected	All models.

### Example

This example shows how to configure a distribute list numbered 2 to use an access list named `acc_list1` for all static routes.



```
config router ospf
    config distribute-list
        edit 2
            set access-list acc_list1
            set protocol static
        end
    end
```

This example shows how to display the settings for distribute list 2.

```
config router ospf
    config distribute-list
        edit 2

        get
    end
```

This example shows how to display the configuration for distribute list 2.

```
config router ospf
    config distribute-list
        edit 2

        show
    end
```

## config neighbor

Access the `config neighbor` subcommand using the `config router ospf` command.

Use this command to manually configure an OSPF neighbor on nonbroadcast networks. OSPF packets are unicast to the specified neighbor address. You can configure multiple neighbors.

## config neighbor command syntax pattern

```
config neighbor
    edit <id_integer>
        set <keyword> <variable>
    end

config neighbor
    edit <id_integer>
        unset <keyword>
    end

config neighbor
    delete <id_integer>
    end

config neighbor
    edit <id_integer>
        get
    end
```

```

config neighbor
  edit <id_integer>
    show
  end

```



**Note:** Only the `ip` keyword is required. All other keywords are optional.

### neighbor command keywords and variables

Keywords and variables	Description	Default	Availability
<code>cost</code> <cost_integer>	Enter the cost to use for this neighbor. The valid range for <code>cost_integer</code> is 1 to 65535.	10	All models.
<code>ip</code> <address_ipv4>	Enter the IP address of the neighbor.	0.0.0.0	All models.
<code>poll-interval</code> <seconds_integer>	Enter the time, in seconds, between hello packets sent to the neighbor in the down state. The value of the poll interval must be larger than the value of the hello interval. The valid range for <code>seconds_integer</code> is 1 to 65535.	10	All models.
<code>priority</code> <priority_integer>	Enter a priority number for the neighbor. The valid range for <code>priority_integer</code> is 0 to 255.	1	All models.

### Example

This example shows how to manually add a neighbor.

```

config router ospf
  config neighbor
    edit 1
      set ip 192.168.21.63
    end
  end
end

```

This example shows how to display the settings for neighbor 1.

```

config router ospf
  config neighbor
    edit 1
      get
    end
  end
end

```

This example shows how to display the configuration for neighbor 1.

```

config router ospf
  config neighbor
    edit 1
      show
    end
  end
end

```

## config network

Access the `config network` subcommand using the `config router ospf` command.

Use this command to identify the interfaces to include in the specified OSPF area. The `prefix` keyword can define one or multiple interfaces.

## config network command syntax pattern

```
config network
  edit <id_integer>
    set <keyword> <variable>
  end

config network
  edit <id_integer>
    unset <keyword>
  end

config network
  delete <id_integer>
  end

config network
  edit <id_integer>
    get
  end

config network
  edit <id_integer>
    show
  end
```

## network command keywords and variables

Keywords and variables	Description	Default	Availability
<code>area &lt;id_ipv4&gt;</code>	The ID number of the area to be associated with the prefix.	No default.	All models.
<code>prefix &lt;address_ipv4mask&gt;</code>	Enter the IP address and netmask for the OSPF network.	No default.	All models.

## Example

Use the following command to enable OSPF for the interfaces attached to networks specified by the IP address 10.0.0.0 and the netmask 255.255.255.0 and to add these interfaces to area 10.1.1.1.

```
config router ospf
  config network
    edit 2
      set area 10.1.1.1
      set prefix 10.0.0.0 255.255.255.0
    end
  end
```

This example shows how to display the settings for network 2.

```
config router ospf
    config network
        edit 2
    get
end
```

This example shows how to display the configuration for network 2.

```
config router ospf
    config network
        edit 2
    show
end
```

### config ospf-interface

Access the `config ospf-interface` subcommand using the `config router ospf` command.

Use this command to change interface related OSPF settings.

### config ospf-interface command syntax pattern



**Note:** The `<interface-name_str>` variable in the syntax pattern below represents a descriptive name for this OSPF configuration. To set the FortiGate interface that this configuration will apply to, use the `interface <name_str>` keyword and variable in the table below.

```
config ospf-interface
    edit <interface-name_str>
        set <keyword> <variable>
    end

config ospf-interface
    edit <interface-name_str>
        unset <keyword>
    end

config ospf-interface
    delete <interface-name_str>
end

config ospf-interface
    edit <interface-name_str>
    get
end

config ospf-interface
    edit <interface-name_str>
    show
end
```



**Note:** The `interface` and `ip` keywords are required. All other keywords are optional.

## ospf-interface command keywords and variables

Keywords and variables	Description	Default	Availability
authentication {md5   none   text}	Use the authentication keyword to define the authentication used for OSPF packets sent and received by this interface. If you select none, no authentication is used. If you select text, the authentication key is sent as plain text. If you select md5, the authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the update packet, not the confidentiality of the routing information in the packet. In text mode the key is sent in clear text over the network. Text mode is usually used only to prevent network problems that can occur if an unwanted or misconfigured router is mistakenly added to the network. If you configure authentication for the interface, authentication for areas is not used. All routers on the network must use the same authentication type.	none	All models.
authentication-key <password_str>	Enter the password to use for text authentication. The authentication-key must be the same on all neighboring routers. The maximum length for the authentication-key is 15 characters.	No default.	All models. authentication must be set to text.
cost <cost_integer>	Specify the cost (metric) of the link. The cost is used for shortest path first calculations.	10	All models.
database-filter-out {disable   enable}	Enable or disable flooding LSAs out of this interface.	disable	All models.
dead-interval <seconds_integer>	The time, in seconds, to wait for a hello packet before declaring a router down. The value of the dead-interval should be four times the value of the hello-interval. All routers on the network must use the same value for dead-interval. The valid range for seconds_integer is 1 to 65535.	40	All models.

**ospf-interface command keywords and variables (Continued)**

Keywords and variables	Description	Default	Availability
hello-interval <seconds_integer>	The time, in seconds, between hello packets. All routers on the network must use the same value for hello-interval. The valid range for seconds_integer is 1 to 65535.	10	All models.
interface <name_str>	Enter the name of the interface to associate with this OSPF configuration.	No default.	All models.
ip <address_ipv4>	Enter the IP address of the interface named by the interface keyword. It is possible to apply different OSPF configurations for different IP addresses defined on the same interface. The IP address 0.0.0.0 is not allowed.	No default.	All models.
md5-key <id_integer> <key_str>	Enter the key ID and password to use for MD5 authentication You can add more than one key ID and key pair per interface. However, you cannot unset one key without unsetting all of the keys. The key ID and key must be the same on all neighboring routers. The valid range for id_integer is 1 to 255. key_str is an alphanumeric string of up to 16 characters.	No default.	All models. authentication must be set to md5.
mtu <mtu_integer>	Change the Maximum Transmission Unit (MTU) size included in database description packets sent out this interface. The valid range for mtu_integer is 576 to 65535.	1500	All models.
mtu-ignore {disable   enable}	Use this command to control the way OSPF behaves when the MTU in the sent and received database description packets does not match. When mtu-ignore is enabled, OSPF will stop detecting mismatched MTUs and go ahead and form an adjacency. When mtu-ignore is disabled, OSPF will detect mismatched MTUs and not form an adjacency. mtu-ignore should only be enabled if it is not possible to reconfigure the MTUs so that they match.	disable	All models.

**ospf-interface command keywords and variables (Continued)**

Keywords and variables	Description	Default	Availability
network-type {broadcast   non-broadcast   point-to-multipoint   point-to-point}	Specify the type of network to which the interface is connected.  OSPF supports four different types of network. This command specifies the behavior of the OSPF interface according to the network type.  If you specify the non-broadcast keyword, you must also configure neighbors using <a href="#">"config neighbor" on page 177</a> .	broadcast	All models.
priority <priority_integer>	Set the router priority for this interface.  Router priority is used during the election of a designated router (DR) and backup designated router (BDR).  An interface with router priority set to 0 can not be elected DR or BDR. The interface with the highest router priority wins the election. If there is a tie for router priority, router ID is used.  Point-to-point networks do not elect a DR or BDR; therefore, this setting has no effect on a point-to-point network.  The valid range for <code>priority_integer</code> is 0 to 255.	1	All models.
retransmit-interval <seconds_integer>	The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet.  The valid range for <code>seconds_integer</code> is 1 to 65535.	5	All models.
status {disable   enable}	Enable or disable OSPF on this interface.	enable	All models.
transmit-delay <seconds_integer>	The estimated time, in seconds, required to send a link state update packet on this interface.  OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the interface.  Increase the value for <code>transmit-delay</code> on low speed links.  The valid range for <code>seconds_integer</code> is 1 to 65535.	1	All models.

## Example

This example shows how to assign an OSPF interface configuration named `test` to the interface named `internal` and how to configure text authentication for this interface.

```
config router ospf
    config ospf-interface
        edit test
            set interface internal
            set ip 192.168.20.3
            set authentication text
            set authentication-key a2b3c4d5e
        end
    end
```

This example shows how to display the settings for the OSPF interface configuration named `test`.

```
config router ospf
    config ospf-interface
        edit test
            get
        end
```

This example shows how to display the configuration for the OSPF interface configuration named `test`.

```
config router ospf
    config ospf-interface
        edit test
            show
        end
```

## config redistribute

Access the `config redistribute` subcommand using the `config router ospf` command.

Use the `config redistribute` command to advertise routes learned from RIP, static routes, or a direct connection to the destination network.



### config redistribute command syntax pattern

```

config redistribute {connected | static | rip}
  set <keyword> <variable>
end

config redistribute {connected | static | rip}
  unset <keyword>
end

get router ospf

show router ospf

```

### redistribute command keywords and variables

Keywords and variables	Description	Default	Availability
metric <metric_integer>	Enter the metric to be used for the redistributed routes. The <code>metric integer</code> range is from 1 to 16777214.	10	All models.
metric-type {1   2}	Specify the external link type to be used for the redistributed routes.	2	All models.
routemap <name_str>	Enter the name of the route map to use for the redistributed routes. For information on how to configure route maps, see <a href="#">"Route-map list" on page 157</a> .	No default.	All models.
status {disable   enable}	Enable or disable redistributing routes.	disable	All models.
tag <tag_integer>	Specify a tag for redistributed routes. The valid range for <code>tag_integer</code> is 0 to 4294967295.	0	All models.

### Example

This example shows how to enable route redistribution from RIP, using a metric of 3 and a route map named `rtmp2`.

```

config router ospf
  config redistribute rip
    set metric 3
    set routemap rtmp2
    set status enable
  end
end

```

This example shows how to display the OSPF settings.

```
get router ospf
```

This example shows how to display the OSPF configuration.

```
show router ospf
```

### config summary-address

Access the `config summary-address` subcommand using the `config router ospf` command.

Use this command to summarize external routes for redistribution into OSPF. This command works only for summarizing external routes on an Autonomous System Boundary Router (ASBR). For information on summarization between areas, see [“config range” on page 171](#). By replacing the LSAs for each route with one aggregate route, you reduce the size of the OSPF link-state database.

### config summary-address command syntax pattern

```
config summary-address
  edit <id_integer>
    set <keyword> <variable>
  end

config summary-address
  edit <id_integer>>
    unset <keyword>
  end

config summary-address
  delete <id_integer>
end

get router ospf

show router ospf
```



**Note:** Only the `prefix` keyword is required. All other keywords are optional.

### summary-address command keywords and variables

Keywords and variables	Description	Default	Availability
<code>advertise</code> { <code>disable</code>   <code>enable</code> }	Advertise or suppress the summary route that matches the specified prefix.	<code>enable</code>	All models.
<code>prefix</code> < <code>address_ipv4mask</code> >	Enter the prefix (IP address and netmask) to use for the summary route. The prefix 0.0.0.0 0.0.0.0 is not allowed.	No default.	All models.
<code>tag</code> < <code>tag_integer</code> >	Specify a tag for the summary route. The valid range for <code>tag_integer</code> is 0 to 4294967295.	0	All models.

### Example

This example shows how to summarize routes using the prefix 10.0.0.0 255.0.0.0.

```
config router ospf
  config summary-address
    edit 5
      set prefix 10.0.0.0 255.0.0.0
    end
  end
```

This example shows how to display the OSPF settings.

```
get router ospf
```

This example shows how to display the OSPF configuration.

```
show router ospf
```

## config router static6

Use this command to add, edit, or delete static routes for IPv6 traffic. Add static routes to control the destination of traffic exiting the FortiGate unit. You configure routes by adding destination IP addresses and netmasks and adding gateways for these destination addresses. The gateways are the next hop routers to which to route traffic that matches the destination addresses in the route.

The FortiGate unit assigns routes using a best match algorithm. To select a route for a packet, the FortiGate unit searches through the routing table for a route that best matches the destination address of the packet. If a match is not found, the FortiGate unit routes the packet using the default route.

## Command syntax pattern

```
config router static6
  edit <sequence_integer>
    set <keyword> <variable>
  end

config router static6
  edit <sequence_integer>
    unset <keyword>
  end

config router static6
  delete <sequence_integer>
end

get router static6 [<sequence_integer>]
show router static6 [<sequence_integer>]
```

## static6 command keywords and variables

Keywords and variables	Description	Default	Availability
device <interface-name_str>	The name of the FortiGate interface through which to route traffic.	null	All models. NAT/Route mode only.
dst <destination-address_ipv6mask>	The destination IPV6 address and netmask for this route. Enter ::/0 for the destination IPV6 address and netmask to add a default route.	::/0	All models. NAT/Route mode only.
gateway <gateway-address_ipv6mask>	The IPV6 address of the first next hop router to which this route directs traffic.	::	All models. NAT/Route mode only.

## Example

This example shows how to add an IPV6 static route that has the sequence number 2.

```
config router static6
  edit 2
    set dev internal
    set dst 12AB:0:0:CD30::/60
    set gateway 12AB:0:0:CD30:123:4567:89AB:CDEF
  end
```

This example shows how to display the list of IPV6 static route numbers.

```
get router static6
```

This example shows how to display the settings for IPV6 static route 2.

```
get router static6 2
```

This example shows how to display the IPV6 static route configuration.

```
show router static6
```

This example shows how to display the configuration for IPV6 static route 2.

```
show router static6 2
```

# Firewall

Firewall policies control all traffic passing through the FortiGate unit. Firewall policies are instructions that the FortiGate unit uses to decide what to do with a connection request. When the firewall receives a connection request in the form of a packet, it analyzes the packet to extract its source address, destination address, and service (by port number).

For the packet to be connected through the FortiGate unit, the source address, destination address, and service of the packet must match a firewall policy. The policy directs the firewall action on the packet. The action can be to allow the connection, deny the connection, require authentication before the connection is allowed, or process the packet as an IPSec VPN packet.

Each policy can be individually configured to route connections or apply network address translation (NAT) to translate source and destination IP addresses and ports. You can add IP pools to use dynamic NAT when the firewall translates source addresses. You can use policies to configure port address translation (PAT) through the FortiGate.

You can add protection profiles to firewall policies to apply different protection settings for traffic that is controlled by firewall policies. You can use protection profiles to:

- Configure antivirus protection for HTTP, FTP, IMAP, POP3, and SMTP policies
- Configure web filtering for HTTP policies
- Configure web category filtering for HTTP policies
- Configure spam filtering for IMAP, POP3, and SMTP policies
- Enable IPS for all services
- Enable content archiving to a FortiLog unit for all services

You can also enable traffic logging for a firewall policy so that the FortiGate unit logs all connections that use this policy.

This chapter describes:

- [Policy](#)
- [Address](#)
- [Service](#)
- [Schedule](#)
- [Virtual IP](#)
- [IP pool](#)
- [Protection profile](#)

## Policy

Go to **Firewall > Policy** to add firewall policies to control connections and traffic between FortiGate interfaces, zones, and VLAN subinterfaces.

The firewall matches policies by searching for a match starting at the top of the policy list and moving down until it finds the first match. You must arrange policies in the policy list from more specific to more general. For example, the default policy is a very general policy because it matches all connection attempts. When you create exceptions to that policy, you must add them to the policy list above the default policy. No policy below the default policy will ever be matched.

This section describes:

- [How policy matching works](#)
- [Policy list](#)
- [Policy options](#)
- [Advanced policy options](#)
- [Configuring firewall policies](#)

### How policy matching works

When the FortiGate unit receives a connection attempt at an interface, it selects a policy list to search through for a policy that matches the connection attempt. The FortiGate unit chooses the policy list based on the source and destination addresses of the connection attempt.

The FortiGate unit then starts at the top of the selected policy list and searches down the list for the first policy that matches the connection attempt source and destination addresses, service port, and time and date at which the connection attempt was received. The first policy that matches is applied to the connection attempt. If no policy matches, the connection is dropped. So, as a general rule, always order your firewall policies from most specific to most general.



**Note:** Policies that require authentication must be added to the policy list above matching policies that do not; otherwise, the policy that does not require authentication is selected first.

### Policy list

You can add, delete, edit, re-order, enable, and disable policies in the policy list.

**Figure 79: Sample policy list**

ID	Source	Dest	Schedule	Service	Action	Enable	
▼ internal -> external (2)							
2	Internal_All	External_All	Always	QUAKE	DENY	<input checked="" type="checkbox"/>	
1	Internal_All	External_All	Always	ANY	ACCEPT	<input checked="" type="checkbox"/>	
▼ external -> internal (1)							
3	External_All	Internal_All	Always	SSH	ACCEPT	<input checked="" type="checkbox"/>	

The policy list has the following icons and features.

<b>Create new</b>	Select Create New to add a firewall policy.
<b>ID</b>	The policy identifier. Policies are numbered in the order they are added to the policy list.
<b>Source</b>	The source address or address group to which the policy applies. See <a href="#">"Address" on page 198</a> .
<b>Dest</b>	The destination address or address group to which the policy applies. <a href="#">"Address" on page 198</a> .
<b>Schedule</b>	The schedule that controls when the policy should be active. See <a href="#">"Schedule" on page 211</a> .
<b>Service</b>	The service to which the policy applies. See <a href="#">"Service" on page 203</a> .
<b>Action</b>	The response to make when the policy matches a connection attempt.
<b>Enable</b>	Enable or disable the policy. Enabling the policy makes it available for the firewall to match it to incoming connections.
<b>source -&gt; destination (n)</b>	Policy list headings indicating the traffic to which the policy applies. The list heading is in the format Source -> Destination (n) where n is the number of policies in the list.
	The Delete and Edit/View icons.
	<b>The Insert Policy before icon.</b> Add a new policy above the corresponding policy (the New Policy screen appears).
	The Move to icon. Move the corresponding policy before or after another policy in the list.

**Figure 80: Move to options**



## Policy options

Policy options are configurable when creating or editing a firewall policy.

Figure 81: Standard policy options

Policy has the following standard options:

<b>Interface / Zone</b>	<p><b>Source</b> Select the source interface name to which the policy will apply.</p> <p><b>Destination</b> Select the destination interface name to which the policy will apply. Interfaces and zones are listed and configured in System &gt; Network. See <a href="#">“System network” on page 47</a>.</p>
<b>Address Name</b>	<p><b>Source</b> Select a source address or address group to which the policy will apply.</p> <p><b>Destination</b> Select a destination address or address group to which the policy will apply. Before you can add this address to a policy, you must add it to the destination interface, VLAN subinterface, or zone. For information about adding an address, see <a href="#">“Addresses” on page x</a>. For NAT/Route mode policies where the address on the destination network is hidden from the source network using NAT, the destination can also be a virtual IP that maps the destination address of the packet to a hidden destination address. See <a href="#">“Virtual IP” on page 214</a>. Before you can use an address in a policy, you must add it to the source interface. See <a href="#">“Address” on page 198</a>.</p>
<b>Schedule</b>	Select a schedule that controls when the policy is available to be matched with connections. See <a href="#">“Schedule” on page 211</a> .
<b>Service</b>	Select a service or protocol to which the policy will apply. You can select from a wide range of predefined services or add custom services and service groups. See <a href="#">“Service” on page 203</a> .



<b>Action</b>	<p>Select how you want the firewall to respond when the policy matches a connection attempt.</p> <ul style="list-style-type: none"> <li>• <b>ACCEPT:</b> Select accept to accept connections matched by the policy. You can also configure NAT and Authentication for the policy.</li> <li>• <b>DENY:</b> Select deny to reject connections matched by the policy. The only other policy option that you can configure is Log Traffic, to log the connections denied by this policy.</li> <li>• <b>ENCRYPT:</b> Select encrypt to make this policy an IPSec VPN policy. When encrypt is selected the VPN Tunnel Options appear. You can select an AutoIKE Key or Manual Key VPN tunnel for the policy and configure other IPSec settings. You cannot add authentication to an ENCRYPT policy.</li> </ul>
<b>VPN Tunnel</b>	<p>Select a VPN tunnel for an ENCRYPT policy. You can select an AutoIKE key or Manual Key tunnel.</p> <ul style="list-style-type: none"> <li>• <b>Allow Inbound:</b> Select Allow inbound so that users behind the remote VPN gateway can connect to the source address.</li> <li>• <b>Allow outbound:</b> Select Allow outbound so that users can connect to the destination address behind the remote VPN gateway.</li> <li>• <b>Inbound NAT:</b> Select Inbound NAT to translate the source address of incoming packets to the FortiGate internal IP address.</li> <li>• <b>Outbound NAT:</b> Select Outbound NAT to translate the source address of outgoing packets to the FortiGate external IP address.</li> </ul>
<b>NAT</b>	<p>Select NAT to enable Network Address Translation for the policy. NAT translates the source address and port of packets accepted by the policy. If you select NAT, you can also select Dynamic IP Pool and Fixed Port. NAT is not available in Transparent mode.</p> <ul style="list-style-type: none"> <li>• <b>Dynamic IP Pool:</b> Select Dynamic IP Pool to translate the source address to an address randomly selected from the IP pool. An IP pool dropdown list appears when the policy destination interface is the same as the IP pool interface.</li> </ul> <p>You cannot select Dynamic IP Pool if the destination interface or VLAN subinterface is configured using DHCP or PPPoE. See <a href="#">"IP pool" on page 219</a>.</p> <ul style="list-style-type: none"> <li>• <b>Fixed Port:</b> Select Fixed Port to prevent NAT from translating the source port. Some applications do not function correctly if the source port is changed. If you select Fixed Port, you must also select Dynamic IP Pool and add a dynamic IP pool address range to the destination interface of the policy. If you do not select Dynamic IP Pool, a policy with Fixed Port selected can only allow one connection at a time for this port or service.</li> </ul>
<b>Protection Profile</b>	<p>Select a protection profile to configure how antivirus and IPS protection, web, web content, and spam filtering are applied to the policy. See <a href="#">"Protection profile" on page 222</a>. If you are configuring authentication in the advanced settings, you do not need to choose a protection profile since the user group chosen for authentication are already tied to protection profiles.</p>
<b>Log Traffic</b>	<p>Select Log Traffic to record messages to the traffic log whenever the policy processes a connection. You must also enable traffic log for a logging location (syslog, WebTrends, local disk if available, memory, or FortiLog) and set the logging severity level to Notification or lower. For information about logging see <a href="#">"Log &amp; Report" on page 339</a>.</p>
<b>Advanced</b>	<p>Select advanced to show more options.</p>

## Advanced policy options

Figure 82: Advanced policy options

### Authentication

You must add users and a firewall protection profile to a user group before you can select Authentication. For information about adding and configuring user groups, see [“User group” on page 239](#).

Select Authentication and select one or more user groups to require users to enter a user name and password before the firewall accepts the connection.

Figure 83: Selecting user groups for authentication

You can select Authentication for any service. Users can authenticate with the firewall using HTTP, Telnet, or FTP. For users to be able to authenticate you must add an HTTP, Telnet, or FTP policy that is configured for authentication. When users attempt to connect through the firewall using this policy they are prompted to enter a firewall username and password.

If you want users to authenticate to use other services (for example POP3 or IMAP) you can create a service group that includes the services for which you want to require authentication, as well as HTTP, Telnet, and FTP. Then users could authenticate with the policy using HTTP, Telnet, or FTP before using the other service.

In most cases you should make sure that users can use DNS through the firewall without authentication. If DNS is not available users cannot connect to a web, FTP, or Telnet server using a domain name.

## Traffic Shaping

Traffic Shaping controls the bandwidth available to and sets the priority of the traffic processed by the policy. Traffic Shaping makes it possible to control which policies have the highest priority when large amounts of data are moving through the FortiGate device. For example, the policy for the corporate web server might be given higher priority than the policies for most employees' computers. An employee who needs unusually high-speed Internet access could have a special outgoing policy set up with higher bandwidth.

If you set both guaranteed bandwidth and maximum bandwidth to 0 (zero), the policy does not allow any traffic.

<b>Guaranteed Bandwidth</b>	You can use traffic shaping to guarantee the amount of bandwidth available through the firewall for a policy. Guarantee bandwidth (in Kbytes) to make sure that there is enough bandwidth available for a high-priority service.
<b>Maximum Bandwidth</b>	You can also use traffic shaping to limit the amount of bandwidth available through the firewall for a policy. Limit bandwidth to keep less important services from using bandwidth needed for more important services.
<b>Traffic Priority</b>	Select High, Medium, or Low. Select Traffic Priority so that the FortiGate unit manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections.

## Differentiated Services

Differentiate Services (DiffServ) describes a set of end-to-end Quality of Service (QoS) capabilities. End-to-end QoS is the ability of a network to deliver service required by specific network traffic from one end of the network to another. By configuring DiffServ you configure your network to deliver particular levels of service for different packets based on the QoS specified by each packet.

DiffServ is defined by RFC 2474 and 2475 as enhancements to the IP networking to enable scalable service discrimination in the IP network without the need for per-flow state and signalling at every hop. DiffServ-capable routers sort IP traffic into classes by inspecting the DS field in IPv4 header or the Traffic Class field in the IPv6 header.

You can use the FortiGate DiffServ feature to change the DSCP (Differentiated Services Code Point) value for all packets accepted by a policy. The network uses these DSCP values to classify, mark, shape, and police traffic, and to perform intelligent queuing. DSCP features are applied to traffic by configuring the routers on your network are configured to apply different service levels to packets depending on the DSCP value of packets that they are routing.

You can configure policies to apply DS values for both forward and reverse traffic. These values are optional and may be enabled independently from each other. When both are disabled, no changes to the DS field are made.

<b>Original (forward) DSCP value</b>	Set the DSCP value for packets accepted by the policy. For example, for an Internal->External policy the value is applied to outgoing packets as they exit the external interface and are forwarded to their destination.
<b>Reverse (reply) DSCP value</b>	Set the DSCP value for reply packets. For example, for an Internal->External policy the value is applied to incoming reply packets before they exit the internal interface and returned to the originator.

### Comments

You can add a description or other information about the policy. The comment can be up to 63 characters long, including spaces.

## Configuring firewall policies

Use the following procedures to add, delete, edit, re-order, disable, and enable a firewall policy.

### To add a firewall policy

- 1 Go to **Firewall > Policy**.
- 2 Select Create New.  
You can also select the Insert Policy before icon beside a policy in the list to add the new policy above that policy.
- 3 Select the source and destination interfaces.
- 4 Select the source and destination addresses.
- 5 Configure the policy.  
For information about configuring the policy, see [“Policy options” on page 191](#).
- 6 Select OK to add the policy.
- 7 Arrange policies in the policy list so that they have the results that you expect.  
For information about arranging policies in a policy list, see [“How policy matching works” on page 190](#).

### To delete a policy

- 1 Go to **Firewall > Policy**.
- 2 Select the Delete icon beside the policy you want to delete.
- 3 Select OK.

### To edit a policy

- 1 Go to **Firewall > Policy**.
- 2 Select the Edit icon beside the policy you want to edit.
- 3 Edit the policy as required.
- 4 Select OK.

### To change the position of a policy in the list

- 1 Go to **Firewall > Policy**.
- 2 Select the Move To icon beside the policy you want to move.

- 3 Select the position for the policy.
- 4 Select OK.

#### To disable a policy

Disable a policy to temporarily prevent the firewall from selecting the policy. Disabling a policy does not stop active communications sessions that have been allowed by the policy.

- 1 Go to **Firewall > Policy**.
- 2 Clear the Enable check box beside the policy you want to disable.

#### To enable a policy

- 1 Go to **Firewall > Policy**.
- 2 Select Enable.

## Policy CLI configuration

The `natip` keyword for the `firewall policy` command is used in encrypted (VPN) policies. A `natip` address cannot be added using the web-based manager. You can configure complete firewall policies using from the CLI. See the *FortiGate CLI Reference Guide* for descriptions of all `firewall policy` keywords.



**Note:** This command has more keywords than are listed in this Guide. See the *FortiGate CLI Reference Guide* for a complete list of commands and keywords.

## Command syntax pattern

```
config firewall policy
  edit <id_integer>
    set <keyword> <variable>
  end
```

### firewall policy command keywords and variables

Keywords and variables	Description	Default	Availability
http_retry_count <retry_integer>	Define the number of times to retry establishing an HTTP connection when the connection fails.	0	All models.
natip <address_ipv4mask>	<p>Configure <code>natip</code> for a firewall policy with action set to <code>encrypt</code> and with outbound NAT enabled. Specify the IP address and subnet mask to translate the source address of outgoing packets.</p> <p>Set <code>natip</code> for peer to peer VPNs to control outbound NAT IP address translation for outgoing VPN packets.</p> <p>If you do not use <code>natip</code> to translate IP addresses, the source addresses of outbound VPN packets are translated into the IP address of the FortiGate external interface. If you use <code>natip</code>, the FortiGate unit uses a static mapping scheme to translate the source addresses of VPN packets into corresponding IP addresses on the subnet that you specify. For example, if the source address in the encryption policy is 192.168.1.0/24 and the <code>natip</code> is 172.16.2.0/24, a source address of 192.168.1.7 will be translated to 172.16.2.7</p>	0.0.0.0 0.0.0.0	All models. Encrypt policy, with outbound NAT enabled.

## Address

You can add, edit, and delete firewall addresses as required. You can also organize related addresses into address groups to simplify policy creation.

A firewall address can be configured with a name, an IP address, and a netmask, or a name and IP address range.

You can enter an IP address and netmask using the following formats.

- x.x.x.x/x.x.x.x, for example 64.198.45.0/255.255.255.0
- x.x.x.x/x, for example 64.195.45.0/24

You can enter an IP address range using the following formats.

- x.x.x.x-x.x.x.x, for example 192.168.110.100-192.168.110.120
- x.x.x.[x-x], for example 192.168.110.[100-120]
- x.x.x.\*, for example 192.168.110.\* to represent all addresses on the subnet

This section describes:

- [Address list](#)
- [Address options](#)
- [Configuring addresses](#)
- [Address group list](#)
- [Address group options](#)
- [Configuring address groups](#)

## Address list

You can add addresses to the list and edit existing addresses. The FortiGate unit comes configured with the default 'All' address which represents any IP address on the network.

**Figure 84: Sample address list**

Create New		
Name	Address	
Internal_All	0.0.0.0/0.0.0.0	
External_All	0.0.0.0/0.0.0.0	
DMZ_All	0.0.0.0/0.0.0.0	
External_Sales	1.2.3.4/255.255.255.0	
Internal_MIS	192.168.20.1 - 192.168.20.10	
Internal_Admin	192.168.20.11 - 192.168.20.20	

The address list has the following icons and features.

- Create New** Select Create New to add a firewall address.
- Name** The name of the firewall address.
- Address** The IP address and mask or IP address range of the firewall.  
The Delete and Edit/View icons.

## Address options

Add an address representing an IP address and subnet mask or an IP address range.

**Figure 85: Address options**

**New Address**

Address Name

IP Range/Subnet

Address has the following options:

- Address Name** Enter a name to identify the firewall address. Addresses, address groups, and virtual IPs must all have unique names to avoid confusion in firewall policies.

**Type** Select the type of address. Each type reveals the corresponding fields to configure.

**IP Range/Subnet** Enter the firewall IP address, forward slash, and subnet mask or enter an IP address range separated by a hyphen

An IP/Mask address can represent:

- The address of a subnet (for example, for a class C subnet, IP address: 192.168.20.0 and Netmask: 255.255.255.0).
- A single IP address (for example, IP Address: 192.168.20.1 and Netmask: 255.255.255.255)
- All possible IP addresses (represented by IP Address: 0.0.0.0 and Netmask: 0.0.0.0)

An IP address can be:

- The IP address of a single computer (for example, 192.45.46.45).
- The IP address of a subnetwork (for example, 192.168.1.0 for a class C subnet).
- 0.0.0.0 to represent all possible IP addresses

The netmask corresponds to the type of address that you are adding. For example:

- The netmask for the IP address of a single computer should be 255.255.255.255.
- The netmask for a class A subnet should be 255.0.0.0.
- The netmask for a class B subnet should be 255.255.0.0.
- The netmask for a class C subnet should be 255.255.255.0.
- The netmask for all addresses should be 0.0.0.0

An IP Range address represents:

- A range of IP addresses in a subnet (for example, 192.168.20.1 to 192.168.20.10)



**Note:** IP address: 0.0.0.0 and Netmask: 255.255.255.255 is not a valid firewall address.

## Configuring addresses

### To add an address

- 1 Go to **Firewall > Address**.
- 2 Select Create New.
- 3 Enter a name to identify the address.
- 4 Enter the IP address and netmask or the IP address range.
- 5 Select OK.

### To edit an address

Edit an address to change its IP information. You cannot edit the address name.

- 1 Go to **Firewall > Address > Address**.
- 2 Select the Edit icon beside the address you want to edit.
- 3 Make any required changes.





**Note:** To change the address name you must delete the address and add it again with a new name. To avoid confusion in firewall policies, an address and a virtual IP cannot have the same name.

- 4 Select OK.

**To delete an address**

Deleting an address removes it from the address list. To delete an address that has been added to a policy, you must first remove the address from the policy.

- 1 Go to **Firewall > Address > Address**.
- 2 Select the Delete icon beside the address you want to delete.  
You cannot delete default addresses.
- 3 Select OK.



**Address group list**

You can organize related addresses into address groups to make it easier to configure policies. For example, if you add three addresses and then configure them in an address group, you can configure a single policy using all three addresses.



**Note:** If an address group is included in a policy, it cannot be deleted unless it is first removed from the policy.

**Figure 86: Sample address group list**

Create New		
Group Name	Members	
Group_1	Internal_MIS,Internal_Admin	 
Group_2	Internal_Admin,External_Sales	 

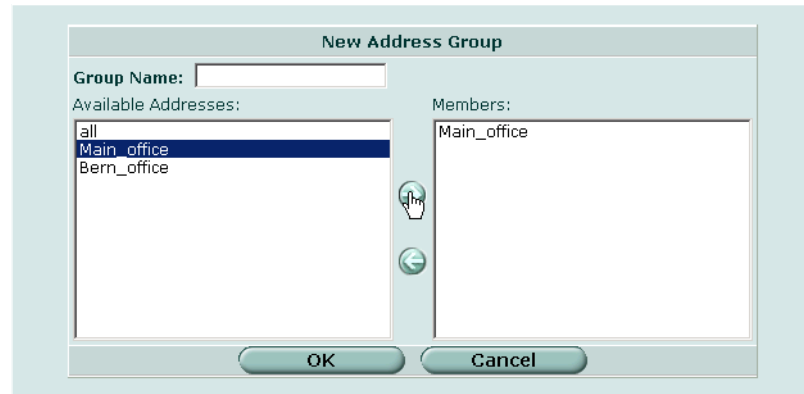
The address group list has the following icons and features.

- Create New** Select Create New to add an address group.
- Group Name** The name of the address group.
- Members** The addresses in the address group.  
The Delete and Edit/View icons.

**Address group options**

Address group options are configurable when creating or editing an address group.

Figure 87: Address group options



Address group has the following options:

<b>Group Name</b>	Enter a name to identify the address group. Addresses, address groups, and virtual IPs must all have unique names to avoid confusion in firewall policies.
<b>Available Addresses</b>	The list of configured and default firewall addresses. Use the arrows to move addresses between the lists.
<b>Members</b>	The list of addresses in the group. Use the arrows to move addresses between the lists.

## Configuring address groups

### To organize addresses into an address group

- 1 Go to **Firewall > Address > Group**.
- 2 Select Create New.
- 3 Enter a group name to identify the address group.
- 4 Select an address from the Available Addresses list and select the right arrow to move the address into the group.
- 5 Repeat step 4 as required to add more addresses to the group.
- 6 Select OK.

### To delete an address group

If an address group is included in a policy, it cannot be deleted unless it is first removed from the policy.

- 1 Go to **Firewall > Address > Group**.
- 2 Select the Delete icon beside the address group you want to delete.
- 3 Select OK.

### To edit an address group

- 1 Go to **Firewall > Address > Group**.
- 2 Select the Edit icon beside the address group you want to modify.

- 3 Make any required changes.



**Note:** To change the address group name you must delete the address group and add it with a new name.

- 4 Select OK.

## Service

Use services to determine the types of communication accepted or denied by the firewall. You can add any of the predefined services to a policy. You can also create custom services and add services to service groups.

This section describes:

- [Predefined service list](#)
- [Custom service list](#)
- [Custom service options](#)
- [Configuring custom services](#)
- [Service group list](#)
- [Service group options](#)
- [Configuring service groups](#)

### Predefined service list

Figure 88: Predefined service list

Predefined		Custom	Group
Name	Detail		
ANY	all		
GRE	ip/47		
AH	ip/51		
ESP	ip/50		
AOL	top/5190-5194		
BGP	top/179		
DHCP	udp/67-68		
DNS	top/53 udp/53		
FINGER	top/79		
FTP	top/21		
GOPHER	top/70		
H323	top/1720,1503 udp/1719		
HTTP	top/80		
HTTPS	top/443		
IKE	udp/500,4500		
INAP	top/143		

The predefined services list has the following icons and features.

<b>Name</b>	The name of the predefined services.
<b>Detail</b>	The protocol for each predefined service.

[Table 21](#) lists the FortiGate predefined firewall services. You can add these services to any policy.

Table 21: FortiGate predefined services

Service name	Description	Protocol	Port
ANY	Match connections on any port. A connection that uses any of the predefined services is allowed through the firewall.	all	all
GRE	Generic Routing Encapsulation. A protocol that allows an arbitrary network protocol to be transmitted over any other arbitrary network protocol, by encapsulating the packets of the protocol within GRE packets.		47
AH	Authentication Header. AH provides source host authentication and data integrity, but not secrecy. This protocol is used for authentication by IPSec remote gateways set to aggressive mode.		51
ESP	Encapsulating Security Payload. This service is used by manual key and AutoIKE VPN tunnels for communicating encrypted data. AutoIKE key VPN tunnels use ESP after establishing the tunnel using IKE.		50
AOL	AOL instant messenger protocol.	tcp	5190-5194
BGP	Border Gateway Protocol routing protocol. BGP is an interior/exterior routing protocol.	tcp	179
DHCP	Dynamic Host Configuration Protocol (DHCP) allocates network addresses and delivers configuration parameters from DHCP servers to hosts.	udp	67
DNS	Domain name service for translating domain names into IP addresses.	tcp	53
		udp	53
FINGER	A network service that provides information about users.	tcp	79
FTP	FTP service for transferring files.	tcp	21
GOPHER	Gopher communication service. Gopher organizes and displays Internet server contents as a hierarchically structured list of files.	tcp	70
H323	H.323 multimedia protocol. H.323 is a standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conferencing data is transmitted across networks.	tcp	1720, 1503
HTTP	HTTP is the protocol used by the word wide web for transferring data for web pages.	tcp	80
HTTPS	HTTP with secure socket layer (SSL) service for secure communication with web servers.	tcp	443
IKE	IKE is the protocol to obtain authenticated keying material for use with ISAKMP for IPSEC.	udp	500
IMAP	Internet Message Access Protocol is a protocol used for retrieving email messages.	tcp	143
Internet-Locator-Service	Internet Locator Service includes LDAP, User Locator Service, and LDAP over TLS/SSL.	tcp	389

**Table 21: FortiGate predefined services (Continued)**

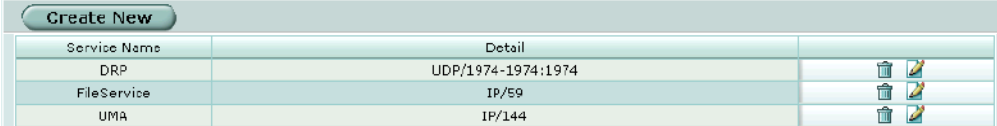
Service name	Description	Protocol	Port
IRC	Internet Relay Chat allows people connected to the Internet to join live discussions.	tcp	6660-6669
L2TP	L2TP is a PPP-based tunnel protocol for remote access.	tcp	1701
LDAP	Lightweight Directory Access Protocol is a set of protocols used to access information directories.	tcp	389
NetMeeting	NetMeeting allows users to teleconference using the Internet as the transmission medium.	tcp	1720
NFS	Network File System allows network users to access shared files stored on computers of different types.	tcp	111, 2049
NNTP	Network News Transport Protocol is a protocol used to post, distribute, and retrieve USENET messages.	tcp	119
NTP	Network time protocol for synchronizing a computer's time with a time server.	tcp	123
OSPF	Open Shortest Path First (OSPF) routing protocol. OSPF is a common link state routing protocol.		89
PC-Anywhere	PC-Anywhere is a remote control and file transfer protocol.	udp	5632
ICMP_ANY	Internet Control Message Protocol is a message control and error-reporting protocol between a host and gateway (Internet).		
PING	ICMP echo request/reply for testing connections to other devices.	icmp	8
TIMESTAMP	ICMP timestamp request messages.	icmp	13
INFO_REQUEST	ICMP information request messages.	icmp	15
INFO_ADDRESS	ICMP address mask request messages.	icmp	17
POP3	Post office protocol is an email protocol for downloading email from a POP3 server.	tcp	110
PPTP	Point-to-Point Tunneling Protocol is a protocol that allows corporations to extend their own corporate network through private tunnels over the public Internet.	tcp	1723
QUAKE	For connections used by the popular Quake multi-player computer game.	udp	26000, 27000, 27910, 27960
RAUDIO	For streaming real audio multimedia traffic.	udp	7070
RLOGIN	Rlogin service for remotely logging into a server.	tcp	513
RIP	Routing Information Protocol is a common distance vector routing protocol.	udp	520
SIP-MSNmessenger	Session Initiation Protocol is used by Microsoft Messenger to initiate an interactive, possibly multimedia session.		







**Table 21: FortiGate predefined services (Continued)**

Service name	Description	Protocol	Port
SMTP	Simple Mail Transfer Protocol is used to send mail between email servers on the Internet.	tcp	25
SNMP	Simple Network Management Protocol is a set of protocols for managing complex networks	tcp	161-162
		udp	161-162
SSH	Secure Shell is a service for secure connections to computers for remote management.	tcp	22
		udp	22
SYSLOG	Syslog service for remote logging.	udp	514
TALK	A protocol supporting conversations between two or more users.	udp	517-518
TCP	All TCP ports.	tcp	0-65535
TELNET	Telnet service for connecting to a remote computer to run commands.	tcp	23
TFTP	Trivial File Transfer Protocol is a simple file transfer protocol similar to FTP but with no security features.	udp	69
UDP	All UDP ports.	udp	0-65535
UUCP	Unix to Unix copy utility, a simple file copying protocol.	udp	540
VDOLIVE	For VDO Live streaming multimedia traffic.	tcp	7000-7010
WAIS	Wide Area Information Server is an Internet search protocol.	tcp	210
WINFRAME	For WinFrame communications between computers running Windows NT.	tcp	1494
X-WINDOWS	For remote communications between an X-Window server and X-Window clients.	tcp	6000-6063

## Custom service list

Add a custom service if you need to create a policy for a service that is not in the predefined service list.

**Figure 89: Sample custom service list**


Create New		
Service Name	Detail	
DRP	UDP/1974-1974:1974	 
FileService	IP/59	 
UMA	IP/144	 

The custom services list has the following icons and features.

- Create New** Select a protocol and then Create New to add a custom service.
- Service Name** The name of the custom service.
- Detail** The protocol and port numbers for each custom service.  
The Delete and Edit/View icons.

## Custom service options

Different options appear depending on the protocol type of custom service you want to define. Choose from TCP, UDP, ICMP, or IP.

### TCP and UDP custom service options

Figure 90: TCP and UDP custom service options

- Name** The name of the TCP or UDP custom service.
- Protocol Type** Select the protocol type of the service you are adding: TCP or UDP. TCP and UDP options are the same.
- Source Port** Specify the Source Port number range for the service by entering the low and high port numbers. If the service uses one port number, enter this number in both the low and high fields.
- Destination Port** Specify the Destination Port number range for the service by entering the low and high port numbers. If the service uses one port number, enter this number in both the low and high fields.

### ICMP custom service options

Figure 91: ICMP custom service options

- Name** The name of the ICMP custom service.
- Protocol Type** Select the protocol type of the service you are adding (ICMP).
- Type** Enter the ICMP type number for the service.
- Code** Enter the ICMP code number for the service if required.

## IP custom service options

Figure 92: IP custom service options



The screenshot shows a dialog box titled "New Custom Service". It has three input fields: "Name" (a text box), "Protocol Type" (a dropdown menu with "IP" selected), and "Protocol Number" (a text box with "0" entered). At the bottom of the dialog are two buttons: "OK" and "Cancel".

**Name** The name of the IP custom service.

**Protocol Type** Select the protocol type of the service you are adding: IP.

**Protocol Number** The IP protocol number for the service.

## Configuring custom services

### To add a custom TCP or UDP service

- 1 Go to **Firewall > Service > Custom**.
- 2 Select Create New.
- 3 Enter a name for the new custom TCP or UDP service.
- 4 Select TCP or UDP as the Protocol Type.
- 5 Specify Source and Destination Port number ranges for the service by entering the low and high port numbers. If the service uses one port number, enter this number in both the low and high fields.
- 6 Select OK.  
You can now add this custom service to a policy.

### To add a custom ICMP service

- 1 Go to **Firewall > Service > Custom**.
- 2 Select Create New.
- 3 Enter a name for the new custom ICMP service.
- 4 Select ICMP as the Protocol Type.
- 5 Enter the ICMP type number and code number for the service.
- 6 Select OK.  
You can now add this custom service to a policy.

### To add a custom IP service

- 1 Go to **Firewall > Service > Custom**.
- 2 Select Create New.
- 3 Enter a name for the new custom IP service.
- 4 Select IP as the Protocol Type.
- 5 Enter the IP protocol number for the service.



- 6 Select OK.  
You can now add this custom service to a policy.

#### To delete a custom service

- 1 Go to **Firewall > Service > Custom**.
- 2 Select the Delete icon beside the service you want to delete.
- 3 Select OK.

#### To edit a custom service

- 1 Go to **Firewall > Service > Custom**.
- 2 Select the Edit icon beside the service you want to edit.
- 3 Modify the custom service as required.



**Note:** To change the custom service name you must delete the service and add it with a new name.

- 4 Select OK.

## Service group list

To make it easier to add policies, you can create groups of services and then add one policy to allow or block access for all the services in the group. A service group can contain predefined services and custom services in any combination. You cannot add service groups to another service group.

**Figure 93: Sample service group list**

Create New		
Group Name	Members	
Group_1	Internal_MIS,Internal_Admin	 
Group_2	Internal_Admin,External_Sales	 

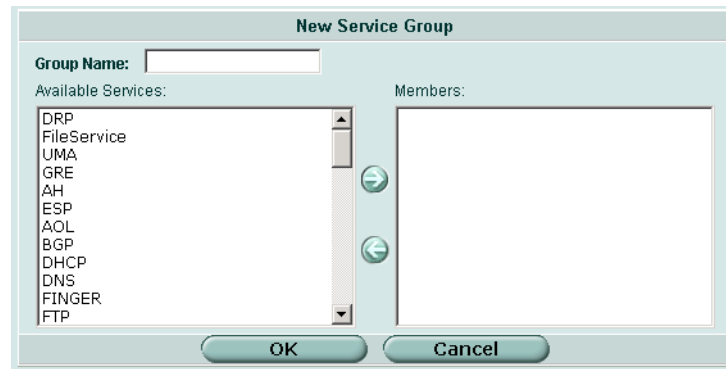
The service group list has the following icons and features.

- Create New** Select Create New to add a service group.
- Group Name** The name to identify the service group.
- Members** The services added to the service group.  
The Delete and Edit/View icons.

## Service group options

Service group options are configurable when creating or editing a service group.

Figure 94: Service group options



Service group has the following options.

<b>Group Name</b>	Enter a name to identify the address group.
<b>Available Services</b>	The list of configured and predefined services. Use the arrows to move services between the lists.
<b>Members</b>	The list of services in the group. Use the arrows to move services between the lists.

## Configuring service groups

### To organize services into a service group

- 1 Go to **Firewall > Service > Group**.
- 2 Select Create New.
- 3 Enter a group name to identify the service group.
- 4 Select a service from the Available Services list and select the right arrow to move the service into the group.
- 5 Select OK.

### To delete a service group

If a service group is included in a policy, it cannot be deleted unless it is first removed from the policy.

- 1 Go to **Firewall > Service > Group**.
- 2 Select the Delete icon beside the service group you want to delete.
- 3 Select OK.

### To edit a service group

- 1 Go to **Firewall > Service > Group**.
- 2 Select the Edit icon beside the service group you want to modify.
- 3 Make any required changes.



**Note:** To change the service group name you must delete the service group and add it with a new name.

- 4 Select OK.

## Schedule

Use schedules to control when policies are active or inactive. You can create one-time schedules and recurring schedules.

You can use one-time schedules to create policies that are effective once for the period of time specified in the schedule. Recurring schedules repeat weekly. You can use recurring schedules to create policies that are effective only at specified times of the day or on specified days of the week.



This section describes:

- [One-time schedule list](#)
- [One-time schedule options](#)
- [Configuring one-time schedules](#)
- [Recurring schedule list](#)
- [Recurring schedule options](#)
- [Configuring recurring schedules](#)

### One-time schedule list

You can create a one-time schedule that activates or deactivates a policy for a specified period of time. For example, your firewall might be configured with the default policy that allows access to all services on the Internet at all times. You can add a one-time schedule to block access to the Internet during a holiday period.

**Figure 95: Sample one-time schedule list**

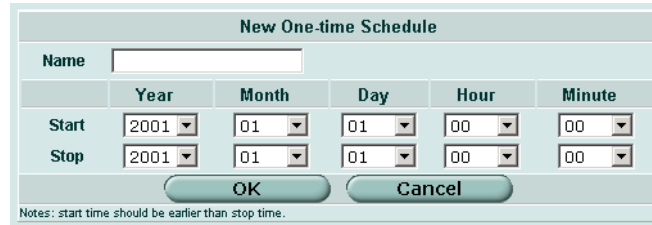
Create New			
Name	Start	Stop	
April_Holiday	2003/04/12 00:00	2003/04/13 07:30	 

The one-time schedule list has the following icons and features.

<b>Create New</b>	Select Create New to add a one-time schedule.
<b>Name</b>	The name of the one-time schedule.
<b>Start</b>	The start date and time for the schedule.
<b>Stop</b>	The stop date and time for the schedule.
	The Delete and Edit/View icons.

## One-time schedule options

Figure 96: One-time schedule options



New One-time Schedule					
Name	<input type="text"/>				
	Year	Month	Day	Hour	Minute
Start	2001	01	01	00	00
Stop	2001	01	01	00	00

Notes: start time should be earlier than stop time.

One-time schedule has the following options.

<b>Name</b>	Enter the name to identify the one-time schedule.
<b>Start</b>	Enter the start date and time for the schedule.
<b>Stop</b>	Enter the stop date and time for the schedule.

## Configuring one-time schedules

### To add a one-time schedule

- 1 Go to **Firewall > Schedule > One-time**.
- 2 Select Create New.
- 3 Type a name for the schedule.
- 4 Select the start date and time for the schedule.  
Set start and stop time to 00 for the schedule to be active for the entire day. One-time schedules use a 24-hour clock.
- 5 Set the Stop date and time for the schedule.
- 6 Select OK.

### To delete a one-time schedule

- 1 Go to **Firewall > Schedule > One-time**.
- 2 Select the Delete icon beside the one-time schedule you want to delete.
- 3 Select OK.

### To edit a one-time schedule

- 1 Go to **Firewall > Schedule > One-time**.
- 2 Select the Edit icon beside the one-time schedule you want to modify.
- 3 Modify the schedule as required.



**Note:** To change the one-time schedule name you must delete the schedule and add it with a new name.

- 4 Select OK to save the changes.

## Recurring schedule list

You can create a recurring schedule that activates or deactivates policies at specified times of the day or on specified days of the week. For example, you might want to prevent game play during working hours by creating a recurring schedule.



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

**Figure 97: Sample recurring schedule list**

Create New				
Name	Day	Start	Stop	
Always	SMTWTF-	00:00	00:00	
Quake	-MTWTF-	08:00	18:00	
NoAccess	-MTWTF-	07:30	05:30	
Weekend	S-----S	00:00	00:00	

The recurring schedule list has the following icons and features.

- Create New** Select Create New to add a recurring schedule.
- Name** The name of the recurring schedule.
- Day** The initials of the days of the week on which the schedule is active.
- Start** The start time of the recurring schedule.
- Stop** The stop time of the recurring schedule.
- The Delete and Edit/View icons.

## Recurring schedule options

**Figure 98: Recurring schedule options**

**New Recurring Schedule**

Name

Day	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start	Hour	<input type="text" value="00"/>	Minute	<input type="text" value="00"/>			
Stop	Hour	<input type="text" value="00"/>	Minute	<input type="text" value="00"/>			

Notes: If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will run for 24 hours.

Recurring schedule has the following options.

- Name** Enter the name to identify the recurring schedule.
- Select** Select the days of the week that you want the schedule to be active.
- Start** Select the start time for the recurring schedule.
- Stop** Select the stop time for the recurring schedule.

## Configuring recurring schedules

### To add a recurring schedule

- 1 Go to **Firewall > Schedule > Recurring**.
- 2 Select Create New.
- 3 Enter a name for the schedule.
- 4 Select the days of the week that you want the schedule to be active.
- 5 Set the Start and Stop time for the recurring schedule.  
Recurring schedules use a 24-hour clock.
- 6 Select OK.

### To delete a recurring schedule

- 1 Go to **Firewall > Schedule > Recurring**.
- 2 Select the Delete icon beside the recurring schedule you want to delete.
- 3 Select OK.

### To edit a recurring schedule

- 1 Go to **Firewall > Schedule > Recurring**.
- 2 Select the Edit icon beside the recurring schedule you want to modify.
- 3 Modify the schedule as required.



**Note:** To change the one-time schedule name you must delete the schedule and add it with a new name.

- 4 Select OK.

## Virtual IP

Use virtual IPs to access IP addresses on a destination network that are hidden from the source network by NAT security policies. To allow connections between these networks, you must create a mapping between an address on the source network and the real address on the destination network. This mapping is called a virtual IP.

For example, if the computer hosting your web server is located on your DMZ network, it could have a private IP address such as 10.10.10.3. To get packets from the Internet to the web server, you must have an external address for the web server on the Internet. You must then add a virtual IP to the firewall that maps the external IP address of the web server to the actual address of the web server on the DMZ network. To allow connections from the Internet to the web server, you must then add an external->DMZ firewall policy and set Destination to the virtual IP.

You can create three types of virtual IPs:

- Static NAT** Used to translate an address on a source network to a hidden address on a destination network. Static NAT translates the source address of return packets to the address on the source network.
- Port Forwarding** Used to translate an address and a port number on a source network to a hidden address and, optionally, a different port number on a destination network. Using port forwarding you can also route packets with a specific port number and a destination address that matches the IP address of the interface that receives the packets. This technique is called port forwarding or port address translation (PAT). You can also use port forwarding to change the destination port of the forwarded packets.
- Dynamic port forwarding** Similar to port forwarding, dynamic port forwarding is used to translate any address and a specific port number on a source network to a hidden address and, optionally a different port number on a destination network.



**Note:** The maximum number of virtual IPs is 1024.

This section describes:

- [Virtual IP list](#)
- [Virtual IP options](#)
- [Configuring virtual IPs](#)

## Virtual IP list

**Figure 99: Sample virtual IP list**

Create New					
Name	IP	Service Port	Map to IP	Map to Port	
Finance	interne/200.3.2.1	tcp/25	192.168.100.100	tcp/25	
Everyone	dmz/na/203.202.201.0		192.168.100.0		

The virtual IP list has the following icons and features.

- Create New** Select Create New to add a virtual IP.
  - Name** The name of the virtual IP.
  - IP** The external IP address mapped to an address on the destination network.
  - Service Port** The external port number of the service from the IP.
  - Map to IP** The real IP address on the destination network.
  - Map to Port** The port number added to packets when they are forwarded (not required).
- The Delete and Edit/View icons.

## Virtual IP options

Different options appear depending on the type of virtual IP you want to define. Choose from Static NAT or port forwarding.

Figure 100:Virtual IP options; static NAT

The screenshot shows the 'Add New Virtual IP Mapping' dialog box. It has the following fields and options:

- Name:** A text input field.
- External Interface:** A dropdown menu with 'internal' selected.
- Type:** Radio buttons for 'Static NAT' (selected) and 'Port Forwarding'.
- External IP Address:** A text input field.
- Map to IP:** A text input field.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

Figure 101:Virtual IP options; port forwarding

The screenshot shows the 'Add New Virtual IP Mapping' dialog box for port forwarding. It has the following fields and options:

- Name:** A text input field.
- External Interface:** A dropdown menu with 'internal' selected.
- Type:** Radio buttons for 'Static NAT' and 'Port Forwarding' (selected).
- External IP Address:** A text input field.
- External Service Port:** A text input field.
- Map to IP:** A text input field.
- Map to Port:** A text input field.
- Protocol:** Radio buttons for 'TCP' (selected) and 'UDP'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

Virtual IP has the following options.

<b>Name</b>	Enter the name to identify the virtual IP. Addresses, address groups, and virtual IPs must all have unique names to avoid confusion in firewall policies.
<b>External Interface</b>	Select the virtual IP external interface from the list.
<b>Type</b>	Select Static NAT or Port Forwarding.
<b>External IP Address</b>	Enter the external IP address that you want to map to an address on the destination network. To configure dynamic port forwarding, set the external IP address to 0.0.0.0.
<b>External Service Port</b>	Enter the external service port number that you want to configure port forwarding for. (Port forwarding only.)
<b>Map to IP</b>	Enter the real IP address on the destination network.
<b>Map to Port</b>	Enter the port number to be added to packets when they are forwarded. (Port forwarding only.)
<b>Protocol</b>	Select the protocol (TCP or UDP) that you want the forwarded packets to use. (Port forwarding only.)

## Configuring virtual IPs

### To add a static NAT virtual IP

- 1 Go to **Firewall > Virtual IP**.
- 2 Select **Create New**.
- 3 Enter a name for the virtual IP.



- 4 Select the virtual IP External Interface from the list.  
The external interface is connected to the source network and receives the packets to be forwarded to the destination network. You can select any firewall interface or a VLAN subinterface. You can set the virtual IP external interface to any FortiGate interface. [Table 22 on page 217](#) contains example virtual IP external interface settings and describes the policies to which you can add the resulting virtual IP.
- 5 Select Static NAT.
- 6 Enter the External IP Address that you want to map to an address on the destination network.  
For example, if the virtual IP provides access from the Internet to a web server on a destination network, the external IP address must be a static IP address obtained from your ISP for your web server. This address must be a unique address that is not used by another host and cannot be the same as the IP address of the external interface selected in step 4. However, the external IP address must be routed to the selected interface. The virtual IP address and the external IP address can be on different subnets.
- 7 Enter the Map to IP address to which to map the external IP address. For example, the IP address of a web server on an internal network.



**Note:** The firewall translates the source address of outbound packets from the host with the Map to IP address to the virtual IP External IP Address, instead of the firewall external address.

- 8 Select OK.  
You can now add the virtual IP to firewall policies.

**Table 22: Virtual IP external interface examples**

External Interface	Description
<b>internal</b>	To map an internal address to an external or DMZ address. Also to map an internal address to an address on a network connected to a VLAN subinterface or connected to a network in a zone. If you select internal, the static NAT virtual IP can be added to policies for connections from the internal interface or a zone containing the internal interface to any other interface, VLAN subinterface, or zone.
<b>external</b>	To map an external address to an internal or DMZ address. Also to map an external address to an address on a network connected to a VLAN subinterface or connected to a network in a zone. If you select external, the static NAT virtual IP can be added to policies for connections from the external interface or a zone containing the external interface to any other interface, VLAN subinterface, or zone.

**To add port forwarding virtual IPs**

- 1 Go to **Firewall > Virtual IP**.
- 2 Select Create New.
- 3 Enter a name for the port forwarding virtual IP.

- 4** Select the virtual IP External Interface from the list.  
The external interface is connected to the source network and receives the packets to be forwarded to the destination network.  
You can select any firewall interface or a VLAN subinterface.
- 5** Select Port Forwarding.
- 6** Enter the External IP Address that you want to map to an address on the destination interface.  
You can set the external IP address to the IP address of the external interface selected in step 4 or to any other address.  
For example, if the virtual IP provides access from the Internet to a server on your internal network, the external IP address must be a static IP address obtained from your ISP for this server. This address must be a unique address that is not used by another host. However, this address must be routed to the external interface selected in step 4. The virtual IP address and the external IP address can be on different subnets.
- 7** Enter the External Service Port number for which you want to configure port forwarding.  
The external service port number must match the destination port of the packets to be forwarded. For example, if the virtual IP provides access from the Internet to a web server, the external service port number is 80 (the HTTP port).
- 8** Enter the Map to IP address to which to map the external IP address. For example, the IP address of a web server on an internal network.
- 9** Enter the Map to Port number to be added to packets when they are forwarded.  
If you do not want to translate the port, enter the same number as the External Service Port.
- 10** Select OK.

#### **To add a dynamic port forwarding virtual IP**

- 1** Go to **Firewall > Virtual IP**.
- 2** Select Create New.
- 3** Enter a name for the dynamic port forwarding virtual IP.
- 4** Select the virtual IP External Interface from the list.  
The external interface is connected to the source network and receives the packets to be forwarded to the destination network.  
You can select any firewall interface or a VLAN subinterface.
- 5** Select Port Forwarding.
- 6** Set the External IP Address to 0.0.0.0.  
The 0.0.0.0 External IP Address matches any IP address.
- 7** Enter the External Service Port number for which you want to configure dynamic port forwarding.  
The external service port number must match the destination port of the packets to be forwarded. For example, if the virtual IP provides PPTP passthrough access from the Internet to a PPTP server, the external service port number should be 1723 (the PPTP port).

- 8 Enter the Map to IP address to which to map the external IP address. For example, the IP address of a PPTP server on an internal network.
- 9 Enter the Map to Port number to be added to packets when they are forwarded. If you do not want to translate the port, enter the same number as the External Service Port.
- 10 Select OK.

#### To delete a virtual IP

- 1 Go to **Firewall > Virtual IP**.
- 2 Select the Delete icon beside the virtual IP you want to delete.
- 3 Select OK.

#### To edit a virtual IP

- 1 Go to **Firewall > Virtual IP**.
- 2 Select the Edit icon beside the virtual IP you want to modify.
- 3 Select OK.

## IP pool

An IP pool (also called a dynamic IP pool) is a range of IP addresses added to a firewall interface. You can enable Dynamic IP Pool in a firewall policy to translate the source address of outgoing packets to an address randomly selected from the IP pool. An IP pool list appears when the policy destination interface is the same as the IP pool interface.

You can add an IP pool if you want to add NAT mode policies that translate source addresses to addresses randomly selected from the IP pool rather than being limited to the IP address of the destination interface.

If you add an IP pool to the internal interface, you can select Dynamic IP pool for policies with the internal interface as the destination. For example, you can add IP pools to External->Internal and DMZ->Internal policies.

You can add multiple IP pools to any interface and select the IP pool to use when configuring a firewall policy.

You can enter an IP address range using the following formats.

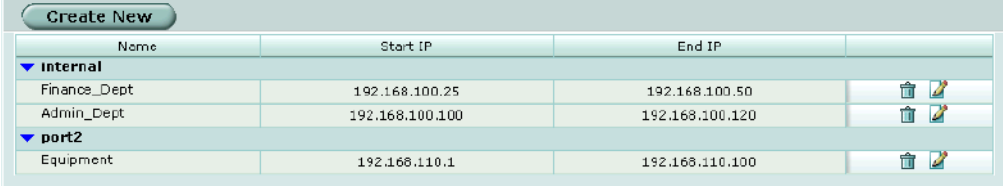
- x.x.x.x-x.x.x.x, for example 192.168.110.100-192.168.110.120
- x.x.x.[x-x], for example 192.168.110.[100-120]







This section describes:

- [IP pool list](#)
- [IP pool options](#)
- [Configuring IP pools](#)
- [IP Pools for firewall policies that use fixed ports](#)
- [IP pools and dynamic NAT](#)

## IP pool list

Figure 102: Sample IP pool list



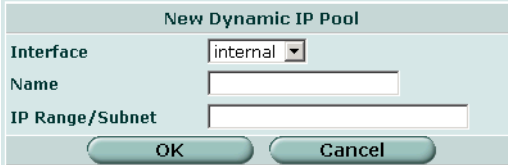
Name	Start IP	End IP	
<b>Internal</b>			
Finance_Dept	192.168.100.25	192.168.100.50	 
Admin_Dept	192.168.100.100	192.168.100.120	 
<b>port2</b>			
Equipment	192.168.110.1	192.168.110.100	 

The IP pool list has the following icons and features.

- Create New** Select Create New to add an IP pool.
- Start IP** The start IP defines the start of an address range.
- End IP** The end IP defines the end of an address range.
- The Delete and Edit/View icons.

## IP pool options

Figure 103: IP pool options



Virtual IP has the following options.

- Interface** Select the interface to which to add an IP pool.
- Name** Enter a name for the IP pool.
- IP Range/Subnet** Enter the IP address range for the IP pool.

## Configuring IP pools

### To add an IP pool

- 1 Go to **Firewall > IP Pool**.
- 2 Select the interface to which to add the IP pool.  
You can select a firewall interface or a VLAN subinterface.
- 3 Select Create New.
- 4 Enter the IP Range for the IP pool.  
The IP range defines the start and end of an address range. The start of the range must be lower than the end of the range. The start and end of the range must be on the same subnet as the IP address of the interface to which you are adding the IP pool.

- 5 Select OK.

#### To delete an IP pool

- 1 Go to **Firewall > IP Pool**.
- 2 Select the Delete icon beside the IP pool you want to delete.
- 3 Select OK.

#### To edit a IP pool

- 1 Go to **Firewall > IP Pool**.
- 2 For the IP pool that you want to edit, select Edit beside it.
- 3 Modify the IP pool as required.
- 4 Select OK to save the changes.

### IP Pools for firewall policies that use fixed ports

Some network configurations do not operate correctly if a NAT policy translates the source port of packets used by the connection. NAT translates source ports to keep track of connections for a particular service. You can select fixed port for NAT policies to prevent source port translation. However, selecting fixed port means that only one connection can be supported through the firewall for this service. To be able to support multiple connections, you can add an IP pool to the destination interface, and then select dynamic IP pool in the policy. The firewall randomly selects an IP address from the IP pool and assigns it to each connection. In this case the number of connections that the firewall can support is limited by the number of IP addresses in the IP pool.

### IP pools and dynamic NAT

You can use IP pools for dynamic NAT. For example, your organization might have purchased a range of Internet addresses but you might have only one Internet connection on the external interface of your FortiGate unit.

You can assign one of your organization's Internet IP addresses to the external interface of the FortiGate unit. If the FortiGate unit is operating in NAT/Route mode, all connections from your network to the Internet appear to come from this IP address.

If you want connections to originate from all your Internet IP addresses, you can add this address range to an IP pool for the external interface. Then you can select Dynamic IP Pool for all policies with the external interface as the destination. For each connection, the firewall dynamically selects an IP address from the IP pool to be the source address for the connection. As a result, connections to the Internet appear to be originating from any of the IP addresses in the IP pool.

## Protection profile

Use protection profiles to apply different protection settings for traffic that is controlled by firewall policies. You can use protection profiles to:

- Configure antivirus protection for HTTP, FTP, IMAP, POP3, and SMTP policies
- Configure web filtering for HTTP policies
- Configure web category filtering for HTTP policies
- Configure spam filtering for IMAP, POP3, and SMTP policies
- Enable IPS for all services

Using protection profiles, you can customize types and levels of protection for different firewall policies.

For example, while traffic between internal and external addresses might need strict protection, traffic between trusted internal addresses might need moderate protection. You can configure policies for different traffic services to use the same or different protection profiles.

Protection profiles can be added to NAT/Route mode and Transparent mode policies.

This section describes:

- [Protection profile list](#)
- [Default protection profiles](#)
- [Protection profile options](#)
- [Configuring protection profiles](#)
- [Profile CLI configuration](#)

### Protection profile list

**Figure 104: Sample list showing the default protection profiles**

Protection Profile	
<a href="#">Create New</a>	
Name	
strict	
scan	
web	
unfiltered	

The IP pool list has the following icons and features.

- Create New** Select Create New to add an IP pool.
- Name** The start IP defines the start of an address range.  
The Delete and Edit/View icons.



**Note:** A protection profile cannot be deleted (and the Delete icon is not visible) if it is selected in a firewall policy or included in a user group.

## Default protection profiles

The FortiGate unit comes preconfigured with four protection profiles.

- Strict** To apply maximum protection to HTTP, FTP, IMAP, POP3, and SMTP traffic. You may not wish to use the strict protection profile under normal circumstances but it is available if you have extreme problems with viruses and require maximum screening.
- Scan** To apply virus scanning to HTTP, FTP, IMAP, POP3, and SMTP traffic. Quarantine is also selected for all content services. On FortiGate models with a hard drive, if antivirus scanning finds a virus in a file, the file is quarantined on the FortiGate hard disk. If required, system administrators can recover quarantined files.
- Web** To apply virus scanning and web content blocking to HTTP traffic. You can add this protection profile to firewall policies that control HTTP traffic.
- Unfiltered** To apply no scanning, blocking or IPS. Use the unfiltered content profile if you do not want to apply content protection to content traffic. You can add this protection profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected.

## Protection profile options

Figure 105: Adding a protection profile



You can configure the following options when creating or editing a protection profile.

- Profile Name** Enter a name for the profile. (New profiles only.)
- Anti-Virus** See [“Configuring antivirus options” on page 224](#).
- Web Filtering** See [“Configuring web filtering options” on page 225](#).
- Web Category Filtering** See [“Configuring web category filtering options” on page 225](#).
- Spam Filtering** See [“Configuring spam filtering options” on page 226](#).
- IPS** See [“Configuring IPS options” on page 227](#).
- Content Archive** See [“Configuring content archive options” on page 227](#).

## Configuring antivirus options

Figure 106: Protection profile antivirus options

▼ Anti-Virus					
	HTTP	FTP	IMAP	POP3	SMTP
Virus Scan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File Block	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Pass Fragmented Emails			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Buffer to Disk	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Oversized File/Email	pass	pass	pass	pass	pass
Add signature to outgoing emails	<input type="checkbox"/> Enable <input type="text" value=""/> (SMTP only)				

The following options are available for antivirus through the protection profile. See [“Antivirus” on page 289](#) for more antivirus configuration options.

<b>Virus Scan</b>	Enable or disable virus scanning (for viruses and worms) for each protocol (HTTP, FTP, IMAP, POP3, SMTP). Grayware, if enabled in Antivirus > Config > Config, is included with the Virus Scan. Heuristic, if enabled in the CLI, is also included with the Virus Scan.
<b>File Block</b>	Enable or disable file pattern blocking for each protocol. You can block files by name, by extension, or any other pattern, giving you the flexibility to block files that may contain harmful content.
<b>Quarantine (models with local disk only)</b>	Enable or disable quarantining for each protocol. You can quarantine suspect files to view them or submit files to Fortinet for analysis.
<b>Pass fragmented emails</b>	Enable or disable passing fragmented email for mail protocols (IMAP, POP3, SMTP). Fragmented email cannot be scanned for viruses.
<b>Oversized file/email</b>	Select block or pass for files and email that exceed configured thresholds for each protocol. To configure the oversized file threshold, go to <b>Antivirus &gt; Config &gt; Config</b> . The maximum threshold for scanning in memory is 10% of the FortiGate unit RAM. <b>Note:</b> For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes less than the configured oversize threshold.
<b>Add signature to outgoing emails</b>	Create and enable a signature to append to outgoing email (SMTP only).



## Configuring web filtering options

Figure 107:Protection profile web filtering options

Web Filtering	
	HTTP
Web Content Block	<input type="checkbox"/>
Web URL Block	<input type="checkbox"/>
Web Exempt List	<input type="checkbox"/>
Web Script Filter	<input type="checkbox"/>
Web resume download block	<input type="checkbox"/>

The following options are available for web filtering through the protection profile. See [“Web filter” on page 309](#) for more web filter configuration options.

- Web Content Block** Enable or disable web page blocking for HTTP traffic based on the banned words and patterns in the content block list.
- Web URL Block** Enable or disable web page filtering for HTTP traffic based on the URL block list.
- Web Exempt List** Enable or disable web page filtering for HTTP traffic based on the URL exempt list. Exempt URLs are not scanned for viruses.
- Web Script Filter** Enable or disable blocking scripts from web pages for HTTP traffic.
- Web resume download block** Enable to block downloading parts of a file that have already been partially downloaded. Enabling this option will prevent the unintentional download of virus files hidden in fragmented files. Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions.

## Configuring web category filtering options

Figure 108:Protection profile web category filtering options (FortiGuard)

Web Category Filtering			
<input type="checkbox"/>	Enable category block (HTTP only)		
<input type="checkbox"/>	Block unrated websites (HTTP only)		
<input type="checkbox"/>	Provide details for blocked HTTP 4xx and 5xx errors (HTTP only)		
<input type="checkbox"/>	Allow websites when a rating error occurs (HTTP only)		
Category	Allow	Block	Monitor
Potentially Liable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Objectionable or Controversial	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Potentially Non-productive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Potentially Bandwidth Consuming	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Potentially Security Violating	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
General Interest	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Business Oriented	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Others	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

The following options are available for web category filtering through the protection profile. See [“Category block” on page 317](#) for more category blocking configuration options.

<b>Enable category block (HTTP only)</b>	Enable FortiGuard category blocking.
<b>Block unrated websites (HTTP only)</b>	Block any web pages that have not been rated by the web filtering service.
<b>Provide details for blocked HTTP 4xx and 5xx errors (HTTP only)</b>	Display a replacement message for 4xx and 5xx HTTP errors. If the error is allowed through then malicious or objectionable sites could use these common error pages to circumvent web category blocking.
<b>Allow websites when a rating error occurs (HTTP only)</b>	Allow web pages that return a rating error from the web filtering service.
<b>Category</b>	The FortiGuard web filtering service provides many categories by which to filter web traffic. You can set the action to take on web pages for each category. Choose from allow, block, or monitor.

## Configuring spam filtering options

Figure 109: Protection profile spam filtering options

▼ Spam Filtering			
	<input checked="" type="checkbox"/> IMAP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> SMTP
IP address FortiShield check	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IP address BWL check	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
RBL & ORDBL check	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HELO DNS lookup	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
E-mail address BWL check	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Return e-mail DNS check	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MIME headers check	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Banned word check	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Spam Action	tagged	tagged	discard ▼
Append to:	<input checked="" type="radio"/> subject <input type="radio"/> MIME	<input checked="" type="radio"/> subject <input type="radio"/> MIME	<input checked="" type="radio"/> subject <input type="radio"/> MIME
Append with:	<input type="text"/>	<input type="text"/>	<input type="text"/>

The following options are available for spam filtering through the protection profile. See [“Spam filter” on page 323](#) for more spam filter configuration options.

<b>IP address FortiShield check</b>	Enable or disable the Fortinet spam filtering IP address blacklist: FortiShield. See <a href="#">“FortiShield” on page 325</a> for a description of this service.
<b>IP address BWL check</b>	Black/white list check. Enable or disable checking incoming IP addresses against the configured spam filter IP address list. (SMTP only.)
<b>RBL &amp; ORDBL check</b>	Enable or disable checking traffic against configured Real-time Blackhole List and Open Relay Database List servers.
<b>HELO DNS lookup</b>	Enable or disable looking up the source domain name (from the SMTP HELO command) in the Domain Name Server.
<b>E-mail address BWL check</b>	Enable or disable checking incoming email addresses against the configured spam filter email address list.

<b>Return e-mail DNS check</b>	Enable or disable checking that the domain specified in the reply-to or from address has an A or MX record.
<b>MIME headers check</b>	Enable or disable checking source MIME headers against the configured spam filter MIME header list.
<b>Banned word check</b>	Enable or disable checking source email against the configured spam filter banned word list.
<b>Spam Action</b>	The action for the spam filter to take. Tagged allows you to append a custom tag to the subject or header of email identified as spam. For SMTP, if you have virus scan or splice (CLI) enabled, you will only be able to discard spam email. (Note that splice is enabled automatically when you enable virus scanning.) Discard immediately drops the connection. Without splice or scanning enabled, you can chose to tag or discard SMTP spam. You can tag email by adding a custom word or phrase to the subject or inserting a MIME header and value into the email header. You can choose to log any spam action in the event log.
<b>Append to</b>	Choose to append the tag to the subject or MIME header of the email identified as spam.
<b>Append with</b>	Enter a word or phrase (tag) to append to email identified as spam. The maximum length is 63 characters.



**Note:** Some popular email clients cannot filter messages based on the MIME header. Check your email client features before deciding how to tag spam.

## Configuring IPS options

Figure 110:Protection profile IPS options

▼ IPS	
IPS Signature	<input type="checkbox"/> Enable (All services)
IPS Anomaly	<input type="checkbox"/> Enable (All services)

The following options are available for IPS through the protection profile. See [“IPS” on page 277](#) for more IPS configuration options.

<b>IPS Signature</b>	Enable or disable signature based intrusion detection and prevention for all protocols.
<b>IPS Anomaly</b>	Enable or disable anomaly based intrusion detection and prevention for all protocols.

## Configuring content archive options

Figure 111:Protection profile content archive options

▼ Content Archive					
	HTTP	FTP	IMAP	POP3	SMTP
Display content meta-information on the system dashboard	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Archive content meta-information to FortiLog	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The following options are available for content archive through the protection profile.

**Display content meta-information on the system dashboard**

Enable to have meta-information for each type of traffic display in the Content Summary section of the FortiGate status page. There you can view statistics for HTTP traffic, FTP traffic, and Email traffic (IMAP, POP3, and SMTP combined).

**Archive content meta-information**

Enable or disable archiving content meta-information to a FortiLog unit for each protocol. Content meta-information can include date and time, source and destination information, request and response size, and scan result. Content archive is only available if FortiLog is enabled under Log&Report > Log Config > Log Settings.

## Configuring protection profiles

### To add a protection profile

If the default protection profiles do not provide the settings you require, you can create custom protection profiles.

- 1 Go to **Firewall > Protection Profile**.
- 2 Select Create New.
- 3 Enter a name for the profile.
- 4 Configure the protection profile options.
- 5 Select OK.



**Note:** If both Virus Scan and File Block are enabled, the FortiGate unit blocks files that match enabled file patterns before they are scanned for viruses.

### To delete a protection profile

- 1 Go to **Firewall > Protection Profile**.
- 2 Select the Delete icon beside the protection profile you want to delete.
- 3 Select OK.

### To edit a protection profile

- 1 Go to **Firewall > Protection Profile**.
- 2 Select the Edit icon beside the protection profile you want to modify.
- 3 Modify the profile as required.



**Note:** To change the one-time schedule name you must delete the schedule and add it with a new name.

- 4 Select OK.

### To add a protection profile to a policy

You can enable protection profiles for firewall policies with action set to allow or encrypt and with service set to ANY, HTTP, FTP, IMAP, POP3, SMTP, or a service group that includes these services.

- 1 Go to **Firewall > Policy**.
- 2 Select a policy list to which you want to add a protection profile.  
For example, to enable network protection for files downloaded from the web by internal network users, select an internal to external policy list.
- 3 Select Create New to add a policy or select Edit for the policy you want to modify.
- 4 Select protection profile.
- 5 Select a protection profile from the list.
- 6 Configure the remaining policy settings, if required.
- 7 Select OK.
- 8 Repeat this procedure for any policies for which you want to enable network protection.

### Profile CLI configuration



**Note:** This guide only describes Command Line Interface (CLI) commands, keywords, or variables (in bold) that are not represented in the web-based manager. For complete descriptions and examples of how to use CLI commands see the *FortiGate CLI Reference Guide*.

Use this command to add, edit or delete protection profiles. Use protection profiles to apply different protection settings for traffic controlled by firewall policies.

#### Command syntax pattern

```
config firewall profile
    edit <profilename_str>
        set <keyword> <variable>
    end

config firewall profile
    edit <profilename_str>
        unset <keyword>
    end

config firewall profile
    delete <profilename_str>
end

get firewall profile [<profilename_str>]
show firewall profile [<profilename_str>]
```

## firewall profile command keywords and variables

Keywords and variables	Description	Default	Availability
<pre>ftp {block content-archive no-content-summary oversize quarantine scan splice}</pre>	<p>Select the actions that this profile will use for filtering FTP traffic for a policy.</p> <ul style="list-style-type: none"> <li>Enter <code>splice</code> to enable the FortiGate unit to simultaneously buffer a file for scanning and upload the file to an FTP server. If a virus is detected, the FortiGate unit stops the upload and attempts to delete the partially uploaded file from the FTP server. To delete the file successfully, the server permissions must be set to allow deletes. When downloading files from an FTP server the FortiGate unit sends 1 byte every 30 seconds to prevent the client from timing out during scanning and download. If a virus is detected, the FortiGate unit stops the download. The user must then delete the partially downloaded file. There should not be enough content in the file to cause any harm. Enabling splice reduces timeouts when uploading and downloading large files. When splice is disabled for ftp, the FortiGate unit buffers the file for scanning before uploading it to the FTP server. If the file is clean, the FortiGate unit will allow the upload to continue.</li> </ul> <p>Enter all the actions you want this profile to use. Use a space to separate the options you enter. If you want to remove an option from the list or add an option to the list, you must retype the list with the option removed or added.</p>	splice	All models.
<pre>http {bannedword block catblock chunkedbypass content-archive no-content-summary oversize quarantine rangeblock scan scriptfilter urlblock url exempt}</pre>	<p>Select the actions that this profile will use for filtering HTTP traffic for a policy.</p> <ul style="list-style-type: none"> <li>Enter <code>chunkedbypass</code> to allow web sites that use chunked encoding for HTTP to bypass the firewall. Chunked encoding means the HTTP message body is altered to allow it to be transferred in a series of chunks. Use this feature at your own risk. Malicious content could enter your network if you allow web content to bypass the firewall.</li> </ul> <p>Enter all the actions you want this profile to use. Use a space to separate the options you enter. If you want to remove an option from the list or add an option to the list, you must retype the list with the option removed or added.</p>	No default.	All models.

### firewall profile command keywords and variables (Continued)

Keywords and variables	Description	Default	Availability
smtp {bannedword block content-archive fragmail no-content-summary oversize quarantine scan spamemailbwl spamfsip spamhdrcheck spamhelodns spamipbwl spamraddrdns spamrbl <b>splice</b> }	<p>Select the actions that this profile will use for filtering SMTP traffic for a policy.</p> <ul style="list-style-type: none"> <li>Enter <code>splice</code> to enable the FortiGate unit to simultaneously scan an email and send it to the SMTP server. If the FortiGate unit detects a virus, it terminates the server connection and returns an error message to the sender, listing the virus name and infected file name. In this mode, the SMTP server is not able to deliver the email if it was sent with an infected attachment. Throughput is higher when <code>splice</code> is enabled. When <code>splice</code> is disabled, the FortiGate unit scans the email first. If the FortiGate unit detects a virus, it removes the infected attachment, adds a customizable message, and sends the email to the SMTP server for delivery. Selecting enable for the <code>splice</code> keyword returns an error message to the sender if an attachment is infected. The receiver does not receive the email or the attachment. When <code>splice</code> is disabled for SMTP, infected attachments are removed and the email is forwarded (without the attachment) to the SMTP server for delivery to the recipient.</li> </ul> <p>Enter all the actions you want this profile to use. Use a space to separate the options you enter. If you want to remove an option from the list or add an option to the list, you must retype the list with the option removed or added.</p>	fragmail splice	All models.

This example shows how to display the settings for the `firewall profile` command.

```
get firewall profile
```

This example shows how to display the settings for the `spammail` profile.

```
get firewall profile spammail
```

This example shows how to display the configuration for the `firewall profile` command.

```
show firewall profile
```

This example shows how to display the configuration for the `spammail` profile.

```
show firewall profile spammail
```





# Users and authentication

You can control access to network resources by defining lists of authorized users, called user groups. To use a particular resource, such as a network or a VPN tunnel, the user must belong to one of the user groups that is allowed access. The user then must correctly enter a user name and password to prove his or her identity. This is called authentication.

You can configure authentication in:

- any firewall policy with Action set to ACCEPT
- IPSec, PPTP and L2TP VPN configurations

When the user attempts to access the resource, the FortiGate unit requests a user name and password. The FortiGate unit can verify the user's credentials locally or using an external LDAP or RADIUS server.

Authentication expires if the user leaves the connection idle for longer than the authentication timeout period.

You need to determine the number and membership of your user groups appropriate to your authentication needs.

## To set up user groups

- 1 If external authentication is needed, configure RADIUS or LDAP servers. See [“RADIUS” on page 235](#) and [“LDAP” on page 236](#).
- 2 Configure local user identities in **User > Local**. For each user, you can choose whether the password is verified by the FortiGate unit, by a RADIUS server or by an LDAP server. See [“Local” on page 234](#).
- 3 Create user groups in **User > User Group**. Add local users as appropriate. See [“User group” on page 239](#).

You can also add a RADIUS or LDAP server to a user group. In this case, all users in the external server's database can authenticate.

This chapter describes:

- [Setting authentication timeout](#)
- [Local](#)
- [RADIUS](#)
- [LDAP](#)
- [User group](#)

## Setting authentication timeout

Authentication timeout controls how long an authenticated firewall connection can be idle before the user must authenticate again.

### To set authentication timeout

- 1 Go to **System > Config > Options**.
- 2 In Auth Timeout, type a number, in minutes.  
The default authentication timeout is 15 minutes.

## Local

Go to **User > Local** to add local user names and configure authentication.

### Local user list

Figure 112:Local user list

Create New		
User Name	Type	
User1	LOCAL	
User2	RADIUS	
User3	LDAP	

- Create New** Add a new local username.
- User Name** The local user name.
- Type** The authentication type to use for this user.  
The Delete and Edit icons.

### Local user options

Figure 113:Local user options

**New User**

**User Name**

Disable

Password

LDAP

Radius

- User Name** Enter the user name.
- Disable** Select Disable to prevent this user from authenticating.
- Password** Select Password to require the user to authenticate using a password. Enter the password that this user must use to authenticate. The password should be at least six characters long.

- LDAP** Select LDAP to require the user to authenticate to an LDAP server. Select the name of the LDAP server to which the user must authenticate. You can only select an LDAP server that has been added to the FortiGate LDAP configuration. See [“LDAP” on page 236](#).
- Radius** Select Radius to require the user to authenticate to a RADIUS server. Select the name of the RADIUS server to which the user must authenticate. You can only select a RADIUS server that has been added to the FortiGate RADIUS configuration. See [“RADIUS” on page 235](#).

### To add a user name and configure authentication

- 1 Go to **User > Local**.
- 2 Select Create New to add a new user name or select the Edit icon to edit an existing configuration.
- 3 Type the User Name.
- 4 Select the authentication type for this user.
- 5 Select OK.

### To delete a user name from the internal database

You cannot delete user names that have been added to user groups. Remove user names from user groups before deleting them.

- 1 Go to **User > Local**.
- 2 Select the Delete icon for the user name that you want to delete.
- 3 Select OK.









**Note:** Deleting the user name deletes the authentication configured for the user.

## RADIUS

If you have configured RADIUS support and a user is required to authenticate using a RADIUS server, the FortiGate unit contacts the RADIUS server for authentication. The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645 you can use the CLI to change the default RADIUS port. For more information see the `config system global` command entry in the *FortiGate CLI Reference Guide*.

### RADIUS server list

Figure 114:RADIUS server list

Create New		
Name	Server Name/IP	
radius1	1.1.1.1	 
Radius2	2.2.2.2	 
Radius3	1.2.1.2	 

- Create New** Add a new RADIUS server.
- Name** The RADIUS server name.

**Server Name/IP** The domain name or IP address of the RADIUS server.  
The Delete and Edit icons.

## RADIUS server options

Figure 115:RADIUS configuration

**Name** Enter a name to identify the RADIUS server.  
**Server Name/IP** Enter the domain name or IP address of the RADIUS server.  
**Server Secret** Enter the RADIUS server secret.

### To configure the FortiGate unit for RADIUS authentication

- 1 Go to **User > RADIUS**.
- 2 Select Create New to add a new RADIUS server or select the Edit icon to edit an existing configuration.
- 3 Enter the Name of the RADIUS server.
- 4 Enter the domain name or IP address of the RADIUS server.
- 5 Enter the RADIUS server secret.
- 6 Select OK.

### To delete a RADIUS server

You cannot delete a RADIUS server that has been added to a user group.

- 1 Go to **User > RADIUS**.
- 2 Select the Delete icon beside the RADIUS server name that you want to delete.
- 3 Select OK.

## LDAP




If you have configured LDAP support and a user is required to authenticate using an LDAP server, the FortiGate unit contacts the LDAP server for authentication. To authenticate with the FortiGate unit, the user enters a user name and password. The FortiGate unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit.

The FortiGate unit supports LDAP protocol functionality defined in RFC2251 for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3.

FortiGate LDAP support does not extend to proprietary functionality, such as notification of password expiration, that is available from some LDAP servers. FortiGate LDAP support does not supply information to the user about why authentication failed.

## LDAP server list

Figure 116:LDAP server list

Create New					
Name	Server Name/IP	Port	Common Name Identifier	Distinguished Name	
LDAP1	2.2.2.2	389	cn	ou=accounts,ou=marketing,dc=fortinet,dc=com	 
LDAP_2	1.32.4.5	389	cn	ou=shipping,dc=fortinet,dc=com	 

- Create New** Add a new LDAP server.
- Server Name/IP** The domain name or IP address of the LDAP server.
- Port** The port used to communicate with the LDAP server.
- Common Name Identifier** The common name identifier for the LDAP server. 20 characters maximum. The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid.
- Distinguished Name** The distinguished name used to look up entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the Common Name Identifier.
- The Delete and Edit icons.

## LDAP server options

Figure 117:LDAP server configuration

New LDAP Server	
Name	<input type="text" value="LDAP_2"/>
Server Name/IP	<input type="text" value="1.32.4.5"/>
Server Port	<input type="text" value="389"/>
Common Name Identifier	<input type="text" value="cn"/>
Distinguished Name	<input type="text" value="ou=shipping,dc=fortinet,dc=com"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- Name** Enter a name to identify the LDAP server.
- Server Name/IP** Enter the domain name or IP address of the LDAP server.
- Server Port** Enter the port used to communicate with the LDAP server. By default LDAP uses port 389.

<b>Common Name Identifier</b>	Enter the common name identifier for the LDAP server. The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid.
<b>Distinguished Name</b>	Enter the distinguished name used to look up entries on the LDAP server. Enter the base distinguished name for the server using the correct X.500 or LDAP format. The FortiGate unit passes this distinguished name unchanged to the server. For example, you could use the following base distinguished name: ou=marketing,dc=fortinet,dc=com where ou is organization unit and dc is domain component. You can also specify multiple instances of the same field in the distinguished name, for example, to specify multiple organization units: ou=accounts,ou=marketing,dc=fortinet,dc=com

#### To configure the FortiGate unit for LDAP authentication:

- 1 Go to **User > LDAP**.
- 2 Select Create New to add a new LDAP server, or select the Edit icon to edit an existing configuration.
- 3 Enter the name of the LDAP server.
- 4 Enter the domain name or IP address of the LDAP server.
- 5 Enter the port used to communicate with the LDAP server.
- 6 Enter the common name identifier for the LDAP server.
- 7 Enter the distinguished name used to look up entries on the LDAP server.
- 8 Select OK.

#### To delete an LDAP server

You cannot delete an LDAP server that has been added to a user group.

- 1 Go to **User > LDAP**.
- 2 Select Delete beside the LDAP server name that you want to delete.
- 3 Select OK.

## User group


To enable authentication, you must add user names, RADIUS servers, and LDAP servers to one or more user groups. You can then assign a firewall protection profile to the user group. You can configure authentication as follows:

- Firewall policies that require authentication:  
You can choose the user groups that are allowed to authenticate with these policies.
- IPSec VPN Phase 1 configurations for dialup users:  
Only users in the selected user group can authenticate to use the VPN tunnel.
- XAuth for IPSec VPN Phase 1 configurations:  
Only user groups in the selected user group can be authenticated using XAuth.
- The FortiGate PPTP configuration:  
Only users in the selected user group can use PPTP.
- The FortiGate L2TP configuration:  
Only users in the selected user group can use L2TP.

When you add user names, RADIUS servers, and LDAP servers to a user group, the order in which they are added determines the order in which the FortiGate unit checks for authentication. If user names are first, then the FortiGate unit checks for a match with these local users. If a match is not found, the FortiGate unit checks the RADIUS or LDAP server. If a RADIUS or LDAP server is added first, the FortiGate unit checks the server and then the local users.

### User group list

Figure 118: User group list

Create New		
Group Name	Members	
Group_1	User1, User2, radius1	 
Group_2	radius1, Radius2	 

- Create New** Add a new user group.
- Group Name** The name of the user group.
- Members** The users, RADIUS servers, or LDAP servers in a user group.
- Protection Profile** The protection profile associated with this user group.
- The Delete and Edit icons.

## User group options

Figure 119:User group configuration

<b>Group Name</b>	Enter the name of the user group.
<b>Available Users</b>	The list of users, RADIUS servers, or LDAP servers that can be added to a user group.
<b>Members</b>	The list of users, RADIUS servers, or LDAP servers added to a user group.
<b>Protection Profile</b>	Select a protection profile for this user group.

### To configure a user group

- 1 Go to **User > User Group**.
- 2 Select Create New to add a new user group, or select the Edit icon to edit an existing configuration.
- 3 Enter a Group Name to identify the user group.
- 4 To add users to the user group, select a user from the Available Users list and select the right arrow to add the name to the Members list.
- 5 To add a RADIUS server to the user group, select a RADIUS server from the Available Users list and select the right arrow to add the RADIUS server to the Members list.
- 6 To add an LDAP server to the user group, select an LDAP server from the Available Users list and select the right arrow to add the LDAP server to the Members list.
- 7 To remove users, RADIUS servers, or LDAP servers from the user group, select a user, RADIUS server, or LDAP server from the Members list and select the left arrow to remove the name, RADIUS server, or LDAP server from the group.
- 8 Select a protection profile from the Protection Profiles list.
- 9 Select OK.



**To delete a user group**

You cannot delete a user group that is included in a firewall policy, a dialup user phase 1 configuration, or a PPTP or L2TP configuration.

- 1 Go to **User > User Group**.
- 2 Select Delete beside the user group that you want to delete.
- 3 Select OK.

## CLI configuration

This guide only covers Command Line Interface (CLI) commands that are not represented in the web-based manager. For complete descriptions and examples of how to use CLI commands see the *FortiGate CLI Reference Guide*.

### peer

Use this command to add or edit the peer certificate information.

#### Command syntax pattern

```
config user peer
  edit <name_str>
    set <keyword> <variable>

config user peer
  edit <name_str>
    unset <keyword>

config user peer
  delete <name_str>

get user peer [<name_str>]

show user peer [<name_str>]
```

#### radius command keywords and variables

Keywords and variables	Description	Default	Availability
ca	Enter the peer Certificate Authority (CA).	No default.	All models.
cn	Enter the peer certificate common name.	No default.	All models.
cn-type {FDQN   email   ipv4   string}	Enter the peer certificate common name type.	string	All models.
subject	Enter the peer certificate name constraints.	No default.	All models.

### Example

This example shows how to add the `branch_office` peer.

```

config user peer
  edit branch_office
    set ca
    set cn
    set cn-type
  end

```

This example shows how to display the list of configured peers.

```
get user peer
```

This example shows how to display the settings for the peer `branch_office`.

```
get user peer branch_office
```

This example shows how to display the configuration for all the peers.

```
show user peer
```

This example shows how to display the configuration for the peer `branch_office`.

```
show user peer branch_office
```

## peergrp

Use this command to add or edit a peer group.

### Command syntax pattern

```

config user peergrp
  edit <name_str>
    set <keyword> <variable>

config user peergrp
  edit <name_str>
    unset <keyword>

config user peergrp
  delete <name_str>

get user peergrp [<name_str>]

show user peergrp [<name_str>]

```

### radius command keywords and variables

Keywords and variables	Description	Default	Availability
member <name_str> [<name_str> [<name_str> [<name_str> ... ]]]	Enter the names of peers to add to the peer group. Separate names by spaces. To add or remove names from the group you must re-enter the whole list with the additions or deletions required.	No default.	All models.

### Example

This example shows how to add peers to the peergrp `EU_branches`.

```
config user peergrp
  edit EU_branches
    set member Sophia_branch Valencia_branch
    Cardiff_branch
  end
```

This example shows how to display the list of configured peer groups.

```
get user peergrp
```

This example shows how to display the settings for the peergrp EU\_branches.

```
get user peergrp EU_branches
```

This example shows how to display the configuration for all the peers groups.

```
show user peergrp
```

This example shows how to display the configuration for the peergrp EU\_branches.

```
show user peergrp EU_branches
```





# VPN

FortiGate units support the following protocols to authenticate and encrypt traffic:

- Internet Protocol Security (IPSec)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer Two Tunneling Protocol (L2TP)

This chapter contains information about the following VPN topics:

- [Phase 1](#)
- [Phase 2](#)
- [Manual key](#)
- [Concentrator](#)
- [Ping Generator](#)
- [Monitor](#)
- [PPTP](#)
- [L2TP](#)
- [Certificates](#)
- [VPN configuration procedures](#)
- [CLI configuration](#)

## Phase 1

The basic phase 1 settings associate IPsec phase 1 parameters with a remote gateway and determine:

- whether the various phase 1 parameters will be exchanged in multiple rounds with encrypted authentication information (main mode) or in a single message with authentication information that is not encrypted (aggressive mode)
- whether a preshared key or digital certificates will be used to authenticate the identities of the two VPN peers
- whether a peer identifier, certificate distinguished name, or group name will be used to identify the remote peer or client when a connection attempt is made

In phase 1, the two VPN peers exchange keys to establish a secure communication channel between them. The advanced P1 Proposal parameters select the encryption and authentication algorithms that are used to generate the keys. Additional advanced phase 1 settings can be selected to ensure the smooth operation of phase 1 negotiations.

### To configure phase 1 settings

- 1 Go to **VPN > IPSEC > Phase 1**.
- 2 Follow the general guidelines in these sections:
  - [“Phase 1 list” on page 246](#)
  - [“Phase 1 basic settings” on page 247](#)
  - [“Phase 1 advanced settings” on page 249](#)

For information about how to choose the correct phase 1 settings for your particular situation, refer to the [FortiGate VPN Guide](#).



**Note:** The procedures in this section assume that you want the FortiGate unit to generate unique IPsec encryption and authentication keys automatically. In situations where a remote VPN peer requires a specific IPsec encryption and/or authentication key, you must configure the FortiGate unit to use manual keys instead. For more information, see [“Manual key” on page 253](#).

## Phase 1 list

Figure 120:IPsec VPN Phase 1 list

Create New				
Gateway Name	Gateway IP	Mode	Encryption Algorithm	
Gateway_1	65.34.56.78	Main	3DES-SHA1 3DES-MD5	
Dialup_gw	Dialup	Main	3DES-SHA1 3DES-MD5	
Dyn-DNS_1	mydomain.com	Main	3DES-SHA1 3DES-MD5	

<b>Create New</b>	Select Create New to create a new phase 1 configuration.
<b>Gateway Name</b>	The names of existing phase 1 configurations.
<b>Gateway IP</b>	The IP address or domain name of a remote peer, or Dialup for a dialup client.
<b>Mode</b>	Main or Aggressive.

**Encryption Algorithm**

The names of the encryption and authentication algorithms used by each phase 1 configuration.

Edit, view, or delete phase 1 configurations.

**Phase 1 basic settings****Figure 121:Phase 1 basic settings**

**Gateway Name** Type a name for the remote VPN peer or client. Enter a name that reflects the origination of the remote connection.

**Remote Gateway** Select the nature of the remote connection:

- If a remote peer with a static IP address will be connecting to the FortiGate unit, select Static IP Address and type the IP address of the remote VPN end point into the IP Address field.
- If one or more dialup clients with dynamic IP addresses will be connecting to the FortiGate unit, select Dialup User.
- If a remote peer that has a domain name and subscribes to a dynamic DNS service will be connecting to the FortiGate unit, select Dynamic DNS and type the domain name of the remote peer into the Dynamic DNS field.

**IP Address** If Static IP Address is selected, type the IP address of the remote peer.

**Dynamic DNS** If Dynamic DNS is selected, type the domain name of the remote peer.

**Mode** Select Main or Aggressive.

- In Main mode, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.
- In Aggressive mode, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted. You must select Aggressive if the FortiGate unit participates in a dynamic DNS configuration.

**Authentication Method** Select Preshared Key or RSA Signature.

- Pre-shared Key** If Preshared Key is selected, type the preshared key that the FortiGate unit will use to authenticate itself to the remote peer during phase 1 negotiations. You must define the same value at the remote peer. The key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.
- Certificate Name** If RSA Signature is selected, select the name of the digital certificate that the FortiGate unit will use to authenticate itself to the remote peer during phase 1 negotiations.
- Peer Options** These options are available to authenticate remote dialup clients or VPN peers with peer IDs or certificate names, depending on the Remote Gateway and Mode settings.
- Select Accept any peer ID to accept the local ID of any remote client or VPN peer.
  - If the remote peer has a domain name and subscribes to a dynamic DNS service, select Accept this peer ID and type the fully qualified domain name of the remote peer. This value must be identical to the value in the Local ID field of the phase 1 remote gateway configuration on the remote peer.
  - To grant access to selected remote peers or clients based on a peer ID, select Accept this peer ID and type the identifier. This value must be identical to the value in the Local ID field of the phase 1 remote gateway configuration on the remote peer or client.
  - To grant access to dialup users based on the name of a dialup group, select Accept peer ID in dialup group and select the name of the group from the list.
  - To grant access to selected remote peers or clients based on a certificate distinguished name, select Accept this peer certificate only and select the name of the certificate from the list. The certificate must be added to the FortiGate configuration through the `config user peer` CLI command before it can be selected. For more information, see the “config user” chapter of the *FortiGate CLI Reference Guide*.
  - To grant access to selected remote peers or clients based on the name of a certificate group, select Accept this peer certificate group only and select the name of the group from the list. The group must be added to the FortiGate configuration through the `config user peer` and `config user peergrp` CLI commands before it can be selected. For more information, see the “config user” chapter of the *FortiGate CLI Reference Guide*.



## Phase 1 advanced settings

Figure 122:Phase 1 advanced settings

### P1 Proposal

Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations.

Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer must be configured to use at least one of the proposals that you define.

You can select any of the following symmetric-key algorithms:

- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
- AES128-A 128-bit block algorithm that uses a 128-bit key.
- AES192-A 128-bit block algorithm that uses a 192-bit key.
- AES256-A 128-bit block algorithm that uses a 256-bit key.

You can select either of the following message digests to check the authenticity of messages during phase 1 negotiations:

- MD5-Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.

To specify a third combination, use the add button beside the fields for the second combination.

<b>DH Group</b>	<p>Select one or more Diffie-Hellman groups from DH group 1, 2, and 5. When using aggressive mode, DH groups cannot be negotiated.</p> <ul style="list-style-type: none"> <li>If both VPN peers have static IP addresses and use aggressive mode, select a single DH group. The setting on the FortiGate unit must be identical to the setting on the remote peer or client.</li> <li>When the VPN peer or client has a dynamic IP address and uses aggressive mode, select up to three DH groups on the FortiGate unit and one DH group on the remote peer or dialup client. The setting on the remote peer or client must be identical to one of the selections on the FortiGate unit.</li> <li>If the VPN peer or client employs main mode, you can select multiple DH groups. At least one of the settings on the remote peer or client must be identical to the selections on the FortiGate unit.</li> </ul>
<b>Keylife</b>	Type the amount of time (in seconds) that will be allowed to pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.
<b>Local ID</b>	<p>If you are using peer IDs for authentication, enter the peer ID that the local FortiGate unit will use to authenticate itself to remote VPN peers.</p> <p>If you are using certificates for authentication, select the distinguished name (DN) of the local certificate.</p>
<b>XAuth</b>	<p>If you select Enable as Client, type the user name and password that the FortiGate unit will need to authenticate itself to the remote peer.</p> <p>To select Enable as Server, you must first create user groups to identify the remote peers and dialup clients that need access to the network behind the FortiGate unit. You must also configure the FortiGate unit to forward authentication requests to an external RADIUS or LDAP authentication server. For information about these topics, see the “Users and Authentication” chapter of the <i>FortiGate Administration Guide</i>. Select a Server Type setting to determine the type of encryption method to use between the FortiGate unit, the XAuth client and the external authentication server, and then select the user group from the User Group list.</p>
<b>Nat-traversal</b>	Enable this option if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared).
<b>Keepalive Frequency</b>	If you enabled NAT traversal, enter a keepalive frequency setting. The value represents an interval from 0 to 900 seconds.
<b>Dead Peer Detection</b>	Enable this option to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required.

## Phase 2

You configure phase 2 settings to specify the parameters for creating and maintaining a VPN tunnel between the FortiGate unit and the remote peer or client. In most cases, you only need to configure the basic phase 2 settings.

### To configure phase 2 settings

- 1 Go to **VPN > IPSEC > Phase 2**.

2 Follow the general guidelines in these sections:

- “Phase 2 list” on page 251
- “Phase 2 basic settings” on page 251
- “Phase 2 advanced options” on page 252

For information about how to choose the correct phase 2 settings for your particular situation, refer to the [FortiGate VPN Guide](#).



**Note:** The procedures in this section assume that you want the FortiGate unit to generate unique IPsec encryption and authentication keys automatically. In situations where a remote VPN peer requires a specific IPsec encryption and/or authentication key, you must configure the FortiGate unit to use manual keys instead. For more information, see “Manual key” on page 253.

## Phase 2 list

Figure 123:IPsec VPN Phase 2 list

Create New					
Tunnel Name	Remote Gateway	Lifetime(sec/kb)	Status	Timeout	
Static_Tunnel_1	65.34.56.78	1800/NA	Down	0	
Dialup_tunnel	Dialup	1800/NA	Unknown	0	
Dyn_DNS_tunnel	mydomain.com	1800/NA	Down	0	

<b>Create New</b>	Select Create New to create a new phase 2 tunnel configuration.
<b>Tunnel Name</b>	The names of existing tunnel configurations.
<b>Remote Gateway</b>	The names of the phase 1 configurations that are associated with the tunnel configurations.
<b>Lifetime (sec/kb)</b>	The tunnel key lifetime.
<b>Status</b>	The current status of the tunnel. If Down, the tunnel is not processing traffic. If Up, the tunnel is currently processing traffic. Unknown is displayed for dialup tunnels.
<b>Timeout</b>	If the tunnel is processing VPN traffic, the Timeout value specifies amount of time left before the next phase 2 key exchange. When the phase 2 key expires, a new key is generated without interrupting service.
	Edit, view or delete phase 2 configurations.

## Phase 2 basic settings

Figure 124:Phase 2 basic settings

**New VPN Tunnel**

Tunnel Name

Remote Gateway

Concentrator

<b>Tunnel Name</b>	Type a name to identify the tunnel configuration.
<b>Remote Gateway</b>	Select the phase 1 configuration to assign to this tunnel. See <a href="#">“Phase 1” on page 246</a> . The phase 1 configuration describes how remote peers or clients will be authenticated on this tunnel, and how the connection to the remote peer or client will be secured.
<b>Concentrator</b>	If the tunnel will be included in a hub-and-spoke configuration, you may select the concentrator from the list. The hub must be added to the FortiGate configuration before it can be selected here. See <a href="#">“Concentrator” on page 256</a> .

## Phase 2 advanced options

Figure 125:Phase 2 advanced settings

**P2 Proposal** Select the encryption and authentication algorithms that will be used to change data into encrypted code. Add or delete encryption and authentication algorithms as required. Select a minimum of one and a maximum of three combinations. The remote peer must be configured to use at least one of the proposals that you define.

You can select any of the following symmetric-key algorithms:

- NULL-Do not use an encryption algorithm.
- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
- AES128-A 128-bit block algorithm that uses a 128-bit key.
- AES192-A 128-bit block algorithm that uses a 192-bit key.
- AES256-A 128-bit block algorithm that uses a 256-bit key.

You can select either of the following message digests to check the authenticity of messages during an encrypted session:

- NULL-Do not use a message digest.
- MD5-Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.

To specify one combination only, set the Encryption and Authentication options of the second combination to NULL. To specify a third combination, use the add button beside the fields for the second combination.

<b>Enable replay detection</b>	Optionally enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.
<b>Enable perfect forward secrecy (PFS)</b>	Enable or disable PFS. Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
<b>DH Group</b>	Select one Diffie-Hellman group (1, 2, or 5). The remote peer or client must be configured to use the same group.
<b>Keylife</b>	Select the method for determining when the phase 2 key expires: Seconds, KBytes, or Both. If you select both, the key expires when either the time has passed or the number of KB have been processed. The range is from 120 to 172800 seconds, or from 5120 to 2147483648 KB.
<b>Autokey Keep Alive</b>	Enable the option if you want the tunnel to remain active when no data is being processed.
<b>DHCP-IPSec</b>	If the FortiGate unit will relay DHCP requests from dialup clients to an external DHCP server, you can select DHCP-IPsec Enable to enable DHCP over IPsec services. The DHCP relay parameters must be configured separately. For more information, see <a href="#">"System DHCP" on page 73</a> .
<b>Internet browsing</b>	If the tunnel will support an Internet-browsing configuration, select the browsing interface from the list.
<b>Quick Mode Identities</b>	Enter the method for choosing selectors for IKE negotiations: <ul style="list-style-type: none"> <li>• To choose a selector from a firewall encryption policy, select Use selectors from policy.</li> <li>• To disable selector negotiation, select Use wildcard selectors.</li> <li>• To specify the firewall encryption policy source and destination IP addresses, select Specify a selector and then select the names of the source and destination addresses from the Source address and Dest address lists. You may optionally specify source and destination port numbers and/or a protocol number.</li> </ul>

## Manual key

If required, you can manually define cryptographic keys for establishing an IPsec VPN tunnel. You would define manual keys in situations where:

- Prior knowledge of the encryption and/or authentication key is required (that is, one of the VPN peers requires a specific IPsec encryption and/or authentication key).
- Encryption and authentication needs to be disabled.

In both cases, you do not specify IPsec phase 1 and phase 2 parameters; you define manual keys on the **VPN > IPSEC > Manual Key** tab instead.

If one of the VPN peers uses specific authentication and encryption keys to establish a tunnel, both VPN peers must be configured to use the same encryption and authentication algorithms and keys.



**Note:** It may not be safe or practical to define manual keys because network administrators must be trusted to keep the keys confidential, and propagating changes to remote VPN peers in a secure manner may be difficult.

It is essential that both VPN peers be configured with matching encryption and authentication algorithms, matching authentication and encryption keys, and complementary Security Parameter Index (SPI) settings.

Each SPI identifies a Security Association (SA). The value is placed in ESP datagrams to link the datagrams to the SA. When an ESP datagram is received, the recipient refers to the SPI to determine which SA applies to the datagram. An SPI must be specified manually for each SA. Because an SA applies to communication in one direction only, you must specify two SPIs per configuration (a local SPI and a remote SPI) to cover bidirectional communications between two VPN peers.



**Caution:** If you are not familiar with the security policies, SAs, selectors, and SA databases for your particular installation, do not attempt the following procedure without qualified assistance.

### To specify manual keys for creating a tunnel

- 1 Go to **VPN > IPSEC > Manual Key** and select Create New.
- 2 Follow the guidelines in these sections:
  - [“Manual key list” on page 254](#)
  - [“Manual key options” on page 255](#)

## Manual key list

Figure 126:IPSec VPN Manual Key list

Create New				
Tunnel Name	Remote Gateway	Encryption Algorithm	Authentication Algorithm	
name	1.1.1.1	3DES	SHA1	 

- Create New** Select Create New to create a new manual key configuration.
- Remote Gateway** The IP address of the remote peer or client.
- Encryption Algorithm** The names of the encryption algorithms used in the configuration.
- Authentication Algorithm** The names of the authentication algorithms used in the configuration.
- Edit, view, or delete manual key configurations.

## Manual key options

Figure 127: Adding a manual key VPN tunnel

New VPN Tunnel	
VPN Tunnel Name	Manual_key_tunnel_1
Local SPI	23333 (Hex)
Remote SPI	223dde (Hex)
Remote Gateway	10.10.10.1
Encryption Algorithm	3DES
Encryption Key (Hex)	***** *****
Authentication Algorithm	MD5
Authentication Key (Hex)	***** *****
Concentrator	

- VPN Tunnel Name** Type a name for the VPN tunnel.
- Local SPI** Type a hexadecimal number (up to 8 characters, 0-9, a-f) that represents the SA that handles outbound traffic on the local FortiGate unit. The valid range is from 0xbb8 to 0xffffffff. This value must match the Remote SPI value in the manual key configuration at the remote peer.
- Remote SPI** Type a hexadecimal number (up to 8 characters, 0-9, a-f) that represents the SA that handles inbound traffic on the local FortiGate unit. The valid range is from 0xbb8 to 0xffffffff. This value must match the Local SPI value in the manual key configuration at the remote peer.
- Remote Gateway** Type the IP address of the public interface to the remote peer. The address identifies the recipient of ESP datagrams.
- Encryption Algorithm** Select one of the following symmetric-key encryption algorithms:
- DES-Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
  - 3DES-Triple-DES, in which plain text is encrypted three times by three keys.
  - AES128-A 128-bit block algorithm that uses a 128-bit key.
  - AES192-A 128-bit block algorithm that uses a 192-bit key.
  - AES256-A 128-bit block algorithm that uses a 256-bit key.
- Encryption Key** If you selected:
- DES, type a 16-character hexadecimal number (0-9, a-f).
  - 3DES, type a 48-character hexadecimal number (0-9, a-f) separated into three segments of 16 characters.
  - AES128, type a 32-character hexadecimal number (0-9, a-f) separated into two segments of 16 characters.
  - AES192, type a 48-character hexadecimal number (0-9, a-f) separated into three segments of 16 characters.
  - AES256, type a 64-character hexadecimal number (0-9, a-f) separated into four segments of 16 characters.

- Authentication Algorithm** Select one of the following message digests:
  - MD5-Message Digest 5 algorithm, which produces a 128-bit message digest.
  - SHA1-Secure Hash Algorithm 1, which produces a 160-bit message digest.
- Authentication Key** If you selected:
  - MD5, type a 32-character hexadecimal number (0-9, a-f) separated into two segments of 16 characters.
  - SHA1, type 40-character hexadecimal number (0-9, a-f) separated into one segment of 16 characters and a second segment of 24 characters.
- Concentrator** If the tunnel will be included in a hub-and-spoke configuration, you may select the concentrator from the list. The hub must be added to the FortiGate configuration before it can be selected here. See [“Concentrator” on page 256](#).

## Concentrator

In a hub-and-spoke configuration, connections to a number of remote peers radiate from a single, central FortiGate unit. Site-to-site connections between the remote peers do not exist; however, VPN tunnels between any two of the remote peers can be established through the FortiGate unit “hub”.

In a hub-and-spoke network, all VPN tunnels terminate at the hub. The peers that connect to the hub are known as “spokes”. The hub functions as a concentrator on the network, managing all VPN connections between the spokes. VPN traffic passes from one tunnel to the other through the hub.

You define a concentrator to include spokes in the hub-and-spoke configuration.

### To define a concentrator

- 1 Go to **VPN > IPSEC > Concentrator**.
- 2 Follow the guidelines in these sections:
  - [“Concentrator list” on page 256](#)
  - [“Concentrator options” on page 257](#)

### Concentrator list

Figure 128:IPSec VPN concentrator list

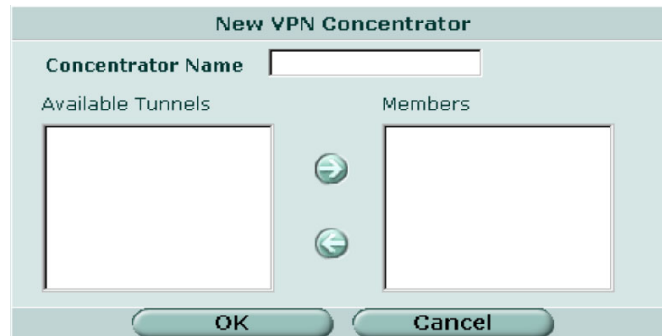
Create New		
Concentrator Name	Members	
Concentrator_1	Tunnel_1, Tunnel_2	
Concentrator_2	Tunnel_3, test3	



<b>Create New</b>	Select Create New to define a new concentrator for an IPSec hub-and-spoke configuration.
<b>Concentrator Name</b>	The names of existing IPSec VPN concentrators.
<b>Members</b>	The tunnels that are associated with the concentrator. Edit, view, or delete concentrators.

## Concentrator options

**Figure 129: Creating a concentrator for a hub-and-spoke configuration**



<b>Concentrator Name</b>	Type a name for the concentrator.
<b>Available Tunnels</b>	A list of defined IPsec VPN tunnels. Select a tunnel from the list and then select the right-pointing arrow. Repeat these steps until all of the tunnels associated with the spokes are included in the concentrator.
<b>Members</b>	A list of tunnels that are members of the concentrator. To remove a tunnel from the concentrator, select the tunnel and select the left-pointing arrow.

## Ping Generator

The ping generator generates traffic in an IPSec VPN tunnel to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, the ping generator is useful in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically—traffic may be suspended while the IP address changes. You may also use the ping generator to troubleshoot network connectivity inside a VPN tunnel.

You can configure settings to generate ping commands through two tunnels simultaneously. The ping interval is fixed at 40 seconds.

The source and destination IP addresses refer to the source and destination addresses of IP packets that are to be transported through the VPN tunnel. When source and destination addresses of 0.0.0.0 are entered, no ping traffic is generated between the source and destination.

### To configure the ping generator

- 1 Go to **VPN > IPSEC > Ping Generator**.

- 2 Select Enable.
- 3 In the Source IP 1 field, type the private IP address or subnet address from which traffic may originate locally (for example, 192.168.20.12 or 192.168.20.0 respectively).
- 4 In the Destination IP 1 field, enter the IP address of a remote computer:
  - For a peer-to-peer configuration, the destination address is the private IP address of a server or host behind the remote VPN peer (for example, 172.16.5.1/32).
  - For a dialup-client or Internet-browsing configuration where the remote VPN client is configured to acquire a virtual IP address, the destination address must correspond to the virtual IP address that can be acquired.
- 5 If you want to enable a second ping generator, repeat Steps 3 and 4 for the Source IP 2 and Destination IP 2 settings.
- 6 Select Apply.

## Ping generator options

Figure 130: Ping generator

Tunnel Keep-Alive Configuration	
<input checked="" type="checkbox"/> Enable	
Source IP 1	192.168.21.200
Destination IP 1	192.168.100.43
Source IP 2	172.16.2.99
Destination IP 2	172.16.34.44
<b>Apply</b>	

- |                         |  |
|-------------------------|--|
| <b>Enable</b>           | Select the option to ping the specified destination address using the specified source address.  |
| <b>Source IP 1</b>      | Enter the IP address from which traffic may originate locally.   |
| <b>Destination IP 1</b> | Enter the IP address of the remote computer to ping.   |
| <b>Source IP 2</b>      | If you want to generate traffic on a second VPN tunnel simultaneously, enter a second IP address from which traffic may originate locally. |
| <b>Destination IP 2</b> | Enter the IP address of the second computer to ping  |

## Monitor

You can use the monitor to view activity on IPsec VPN tunnels and start or stop those tunnels. The display provides a list of addresses, proxy IDs, and timeout information for all active tunnels.

### To view active tunnels

- 1 Go to **VPN > IPSEC > Monitor**.

To interpret the display, see the following sections:

- [“Dialup monitor” on page 259](#)
- [“Static IP and dynamic DNS monitor” on page 259](#)

**To establish or take down a VPN tunnel**

- 1 Go to **VPN > IPSEC > Monitor**.
- 2 In the list of tunnels, select the Bring down tunnel or Bring up tunnel button in the row that corresponds to the tunnel that you want to bring down or up.

If you take down an active tunnel while a dialup client such as FortiClient is still connected, FortiClient will continue to show the tunnel connected and idle. The dialup client must disconnect before another tunnel can be initiated.

**Dialup monitor**

The list of dialup tunnels provides information about the status of tunnels that have been established for dialup clients. The list displays the IP addresses of dialup clients and the names of all active tunnels. The number of tunnels shown in the list can change as dialup clients connect and disconnect.

**Figure 131: Dialup monitor**

Name	Remote gateway	Username	Timeout	Proxy ID Source	Proxy ID Destination
Dialup_tunnel_3	172.20.120.20:500		1746	10.0.0.2	172.20.120.20

**Flush dialup tunnels icon** Stop all dialup tunnels and stop the traffic passing through all dialup tunnels. Dialup users may have to reconnect to establish new VPN sessions.

**Name** The name of the tunnel.

**Remote gateway** The IP address and UDP port of the remote gateway.

**Username** The peer ID, certificate name, or XAuth user name of the dialup client (if a peer ID, certificate name, or XAuth user name was assigned to the dialup client for authentication purposes).

**Timeout** The time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.

**Proxy ID Source** The IP address of the host, server, or private network behind the FortiGate unit. A network range may be displayed if the source address in the firewall encryption policy was expressed as a range of IP addresses.

**Proxy ID Destination** The virtual IP (VIP) address of the dialup client. A range of VIP addresses may be displayed if the destination address in the firewall encryption policy was expressed as a range of VIP addresses.

**Bring down tunnel icon** Stop the current dialup tunnel. The dialup user may have to reconnect to establish a new VPN session.

**Static IP and dynamic DNS monitor**

The list of tunnels provides information about VPN connections to remote peers that have static IP addresses or domain names. You can use this list to view status and IP addressing information for each tunnel configuration. You can also start and stop individual tunnels from the list.

**Figure 132: Static IP and dynamic DNS monitor**

Name	Remote gateway	Timeout	Proxy ID Source	Proxy ID Destination
FG_hidden_FortiLog	192.168.34.56:500	0	0.0.0.0-255.255.255.255	192.168.34.56
FG1toSP1_Tunnel	172.16.20.1:500	0	192.168.22.*	192.168.33.*
FG1toSP2_Tunnel	172.16.30.1:500	0	192.168.22.*	192.168.44.*
Redundant_tunnel	10.10.10.2:500	0		
Redundant_tunnel	10.10.10.1:500	0		

<b>Name</b>	The name of the tunnel.
<b>Remote gateway</b>	The IP address and UDP port of the remote gateway. For dynamic DNS tunnels, the IP address is updated dynamically.
<b>Timeout</b>	The time before the next key exchange. The time is calculated by subtracting the time elapsed since the last key exchange from the keylife.
<b>Proxy ID Source</b>	The IP address of the host, server, or private network behind the FortiGate unit. A network range may be displayed if the source address in the firewall encryption policy was expressed as a range of IP addresses.
<b>Proxy ID Destination</b>	The IP address of the remote peer.
<b>Bring down tunnel icon</b>	Take down the selected VPN tunnel. The remote VPN peer may have to reconnect to establish a new VPN session.
<b>Bring up tunnel icon</b>	Establish the selected VPN tunnel.

## PPTP

FortiGate units support PPTP to tunnel PPP traffic between two VPN peers. Windows or Linux PPTP clients can establish a PPTP tunnel with a FortiGate unit that has been configured to act as a PPTP server. As an alternative, you can configure the FortiGate unit to forward PPTP packets to a PPTP server on the network behind the FortiGate unit.

For information about how to perform these tasks, see [“PPTP configuration procedures” on page 268](#).

### To enable PPTP and specify the PPTP address range

- 1 Go to **VPN > PPTP > PPTP Range**.
- 2 Enable PPTP and specify the address range.

### PPTP range

The PPTP address range is the range of addresses reserved for remote PPTP clients. When the remote PPTP client connects, the FortiGate unit assigns an IP address from a reserved range of IP addresses to the client PPTP interface. The PPTP client uses the assigned IP address as its source address for the duration of the connection.

**Figure 133:PPTP range**

<b>Enable PPTP</b>	You must add a user group before you can select the option.
<b>Starting IP</b>	Type the starting address in the range of reserved IP addresses.
<b>Ending IP</b>	Type the ending address in the range of reserved IP addresses.
<b>User Group</b>	Select the name of the PPTP user group that you defined.
<b>Disable PPTP</b>	Select the option to disable PPTP support.

## L2TP

A FortiGate unit can be configured to act as an L2TP network server. The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP tunnel with the FortiGate unit directly.

For information about how to perform the related tasks, see [“L2TP configuration procedures” on page 268](#).

### To enable L2TP and specify the L2TP address range

- 1 Go to **VPN > L2TP > L2TP Range**.
- 2 Enable L2TP and specify the address range.

### L2TP range

The L2TP address range specifies the range of addresses reserved for remote clients. When a remote client connects to the FortiGate unit, the client is assigned an IP address from this range. Afterward, the FortiGate unit uses the assigned address to communicate with the remote client.

**Figure 134:L2TP range**

<b>Enable L2TP</b>	You must add a user group before you can enable the option.
<b>Starting IP</b>	Type the starting address in the range of reserved IP addresses.
<b>Ending IP</b>	Type the ending address in the range of reserved IP addresses.
<b>User Group</b>	Select the name of the L2TP user group that you defined.
<b>Disable L2TP</b>	Select the option to disable L2TP support.

## Certificates

Digital certificates are downloadable files that you can install on the FortiGate unit and on remote peers and clients for authentication purposes.

An X.509 digital certificate contains information that has been digitally signed by a trusted third party known as a certificate authority (CA). Because CAs can be trusted, the certificates issued by a CA are deemed to be trustworthy.

### To view and manage local certificates

- 1 Go to **VPN > Certificates > Local Certificates**.
- 2 Follow the guidelines in these sections:
  - [“Local certificate list” on page 262](#)
  - [“Certificate request” on page 263](#)
  - [“Importing signed certificates” on page 264](#)







### To import and view CA certificates

- 1 Go to **VPN > Certificates > CA Certificates**.
- 2 For more information, see [“CA certificate list” on page 265](#) and [“Importing CA certificates” on page 265](#).

For detailed information and step-by-step procedures related to obtaining and installing digital certificates, see the [FortiGate VPN Guide](#).

## Local certificate list

Figure 135:Certificate list

Generate		Import	
Name	Subject	Status	
FG-100_Lab	CN = 172.20.120.125	OK	  
User_1	CN = user1@fortinet.com	OK	  

- Generate** Select to generate a local certificate request. See [“Certificate request” on page 263](#).
- Import** Select to import a signed local certificate. See [“Importing signed certificates” on page 264](#).
- Name** The names of existing local certificates and pending certificate requests.
- Subject** The Distinguished Names (DNs) of local signed certificates.
- Status** The status of the local certificate. PENDING designates a certificate request that should be downloaded and signed.
- View Certificate Detail icon** Select to display certificate details such as the certificate name, issuer, subject, and valid certificate dates. See [Figure 136](#).
- Download icon** Select to save a copy of the certificate request to a local computer. Send the request to your CA to obtain a certificate for the FortiGate unit.

**Figure 136:Certificate details**

Certificate Detail Information	
<b>Certificate Name:</b>	FG-100_Lab
<b>Issuer:</b>	C = CA, ST = Ontario, L = Ottawa, O = Fortinet, OU = AutoTest, CN = caserver, emailAddress = caserver@localdomain
<b>Subject:</b>	CN = 172.20.120.125
<b>Valid From:</b>	Nov 10 20:52:49 2004 GMT
<b>Valid To:</b>	Nov 8 20:52:49 2014 GMT

## Certificate request

To obtain a personal or site certificate, you must send a request to a CA that provides digital certificates that adhere to the X.509 standard. The FortiGate unit provides a way for you to generate the request. The generated request includes information such as the FortiGate unit's public static IP address, domain name, or email address.

### To generate a certificate request

- 1 Go to **VPN > Certificates > Local Certificates**.
- 2 Select Generate.

**Figure 137:Generating a certificate signing request**

**Generate Certificate Signing Request**

**Certification Name**

---

**Subject Information**

ID Type

IP

---

**Optional Information**

Organization Unit

Organization

Locality(City)

State/Province

Country

e-mail

---

**Key Type**

**Key Size**

<b>Certification Name</b>	Type a certificate name. Typically, this would be the name of the FortiGate unit.
<b>Subject Information</b>	<p>Enter the information needed to identify the FortiGate unit. Preferably use an IP address or domain name. If this is impossible (such as with a dialup client), use an email address.</p> <ul style="list-style-type: none"> <li>For Host IP, enter the public IP address of the FortiGate unit being certified.</li> <li>For Domain name, enter the fully qualified domain name of the FortiGate unit being certified. Do not include the protocol specification (http://) or any port number or path names.</li> <li>For E-mail, enter the email address of the owner of the FortiGate unit being certified. Typically, email addresses are entered only for clients, not gateways.</li> </ul>
<b>Organization Unit</b>	Name of your department.
<b>Organization</b>	Legal name of your company or organization.
<b>Locality (City)</b>	Name of the city or town where the FortiGate unit is installed.
<b>State/Province</b>	Name of the state or province where the FortiGate unit is installed.
<b>Country</b>	Select the country where the FortiGate unit is installed.
<b>e-mail</b>	Contact email address. The CA may choose to deliver the digital certificate to this address.
<b>Key Type</b>	Only RSA is supported.
<b>Key Size</b>	Select 1024 Bit, 1536 Bit or 2048 Bit. Larger keys are slower to generate but more secure. Not all IPSec VPN products support all three key sizes.

## Importing signed certificates

Your CA will provide you with a signed certificate to install on the FortiGate unit. When you receive the signed certificate from the CA, save the certificate on a PC that has management access to the FortiGate unit.

### To install a signed personal or site certificate

- 1 Go to **VPN > Certificates > Local Certificates**.
- 2 Select Import.

**Figure 138: Importing a signed certificate**





- 3 Browse to the location on the management PC where the certificate has been saved, select the certificate, and then select OK.
- 4 Select OK.



## CA certificate list

Follow the CA instructions to download their root certificate, and then install the root certificate on the FortiGate unit. The installed CA certificates are displayed in the CA certificate list.

Figure 139:CA certificate list

Import		
Name	Subject	
CA_Cert_1	O = Root CA, OU = http://www.cacert.org, CN = CA Cert Signing Authority, emailAddress =	 

<b>Import</b>	Select to import a CA root certificate. See <a href="#">“Importing CA certificates” on page 265</a> .
<b>Name</b>	The names of existing CA root certificates. The FortiGate unit assigns unique names (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on) to the CA certificates when they are imported.
<b>Subject</b>	Information about the CA.
<b>View Certificate Detail icon</b>	Select to display certificate details.
<b>Download icon</b>	Select if you want to save a copy of the CA root certificate to a local computer.

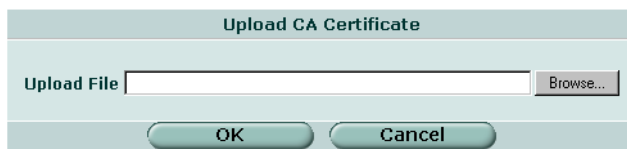
## Importing CA certificates

After you download the root certificate of the CA, save the certificate on a PC that has management access to the FortiGate unit.

### To import a CA root certificate

- 1 Go to **VPN > Certificates > CA Certificates**.
- 2 Select Import.

Figure 140:Importing a CA certificate



- 3 Browse to the location on the management PC where the certificate has been saved, select the certificate, and then select OK.
- 4 Select OK.

## VPN configuration procedures

The [FortiGate VPN Guide](#) uses a task-based approach to provide all of the procedures needed to create different types of VPN configurations. The guide contains the following chapters:

- “Configuring IPsec VPNs” describes how to set up various IPsec VPN configurations.
- “Configuring PPTP VPNs” describes how to configure a PPTP tunnel between a FortiGate unit and a PPTP client.
- “Configuring L2TP VPNs” describes how to configure the FortiGate unit to operate as an L2TP network server.
- “Monitoring and Testing VPN Tunnels” outlines some general monitoring and testing procedures for VPNs.

General high-level procedures are presented here. For details, see the [FortiGate VPN Guide](#).

### IPsec configuration procedures

The following configuration procedures are common to all IPsec VPNs:

- 1 Define the phase 1 parameters that the FortiGate unit needs to authenticate remote peers and establish a secure connection. See [“Phase 1” on page 246](#).
- 2 Define the phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with a remote peer. See [“Phase 2” on page 250](#).
- 3 Define source and destination addresses for the IP packets that are to be transported through the VPN tunnel, and create the firewall encryption policy, which defines the scope of permitted services between the IP source and destination addresses. See [“Adding firewall policies for IPsec VPN tunnels” on page 266](#).



**Note:** Perform Steps 1 and 2 to have the FortiGate unit generate unique IPsec encryption and authentication keys automatically. In situations where a remote VPN peer requires a specific IPsec encryption and/or authentication key, you must configure the FortiGate unit to use manual keys instead of performing Steps 1 and 2. For more information, see [“Manual key” on page 253](#).

### Adding firewall policies for IPsec VPN tunnels

Firewall policies control all IP traffic passing between a source address and a destination address. A firewall encryption policy is needed to allow the transmission of encrypted packets, specify the permitted direction of VPN traffic, and select the VPN tunnel that will be subject to the policy. A single encryption policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

Before you define the policy, you must first specify the IP source and destination addresses.

#### To define an IP source address

- 1 Go to **Firewall > Address** and select Create New.

- 2 In the Address Name field, type a name that represents the local network, server(s), or host(s) from which IP packets may originate on the private network behind the local FortiGate unit.
- 3 In the IP Range/Subnet field, type the corresponding IP address and subnet mask (for example, 172.16.5.0/24 for a subnet, or 172.16.5.1/32 for a server or host) or IP address range (for example, 192.168.10.[80-100]).
- 4 Select OK.

#### To define an IP destination address

- 1 Go to **Firewall > Address** and select Create New.
- 2 In the Address Name field, type a name that represents the remote network, server(s), or host(s) to which IP packets may be delivered.
- 3 In the IP Range/Subnet field, type the corresponding IP address and subnet mask (for example, 192.168.20.0/24 for a subnet, or 192.168.20.2/32 for a server or host), or IP address range (for example, 192.168.20.[10-25]).
- 4 Select OK.

#### To define the firewall encryption policy

- 1 Go to **Firewall > Policy** and select Create New.
- 2 Include appropriate entries as follows:

<b>Interface/Zone</b>	Source Select the local interface to the internal (private) network. Destination Select the local interface to the external (public) network.
<b>Address Name</b>	Source Select the name that corresponds to the local network, server(s), or host(s) from which IP packets may originate. Destination Select the name that corresponds to the remote network, server(s), or host(s) to which IP packets may be delivered. The name may correspond to a VIP-address range for dialup clients.
<b>Schedule</b>	Keep the default setting (always) unless changes are needed to meet specific requirements.
<b>Service</b>	Keep the default setting (ANY) unless changes are needed to meet your specific requirements.
<b>Action</b>	Select ENCRYPT.
<b>VPN Tunnel</b>	Select the name of the phase 2 tunnel configuration to which this policy will apply. Select Allow inbound if traffic from the remote network will be allowed to initiate the tunnel. Select Allow outbound if traffic from the local network will be allowed to initiate the tunnel. Select Inbound NAT to translate the source IP addresses of inbound decrypted packets into the IP address of the FortiGate internal interface. Select Outbound NAT to translate the source address of outbound encrypted packets into the IP address of the FortiGate public interface.

- 3 You may enable a protection profile, and/or event logging, or select advanced settings to shape traffic or differentiate services. See the “Firewall” chapter of the *FortiGate Administration Guide*.
- 4 Select OK.
- 5 Place the policy in the policy list above any other policies having similar source and destination addresses.

## PPTP configuration procedures

If the FortiGate unit will act as a PPTP server, perform the following tasks on the FortiGate unit:

- 1 Create a PPTP user group containing one user for each PPTP client. See “[Users and authentication](#)” on page 233.
- 2 Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect. See “[PPTP range](#)” on page 260.
- 3 Configure the PPTP server.
- 4 Configure the PPTP clients.

To perform Steps 3 and 4, see the *FortiGate VPN Guide*.

To arrange for PPTP packets to pass through the FortiGate unit to an external PPTP server instead, you must:

- 1 Create a PPTP user group containing one user for each PPTP client. See “[Users and authentication](#)” on page 233.
- 2 Enable PPTP on the FortiGate unit and specify the range of addresses that can be assigned to PPTP clients when they connect. See “[PPTP range](#)” on page 260.
- 3 Configure PPTP pass through on the FortiGate unit.
- 4 Configure the PPTP clients.

To perform Steps 3 and 4, see the *FortiGate VPN Guide*.

## L2TP configuration procedures

To configure a FortiGate unit to act as an L2TP network server, perform the following tasks on the FortiGate unit:

- 1 Create an L2TP user group containing one user for each remote client. See “[Users and authentication](#)” on page 233.
- 2 Enable L2TP on the FortiGate unit and specify the range of addresses that can be assigned to remote clients when they connect. See “[L2TP range](#)” on page 261.
- 3 Configure the L2TP server.
- 4 Configure the remote clients.

To perform Steps 3 and 4, see the *FortiGate VPN Guide*.

## CLI configuration

This section provides information about features that must be configured through CLI commands. CLI commands provide additional network options that cannot be configured through the web-based manager. For complete descriptions and examples of how to use CLI commands, see the *FortiGate CLI Reference Guide*.

### ipsec phase1

In the web-based manager, the Dead Peer Detection option can be enabled when you define advanced Phase 1 options. The `config vpn ipsec phase1` CLI command supports additional options for specifying a long and short idle time, a retry count, and a retry interval.

#### Command syntax pattern

```
config vpn ipsec phase1
  edit <name_str>
    set <keyword> <variable>
  end

config vpn ipsec phase1
  edit <name_str>
    unset <keyword>
  end
```

#### ipsec phase1 command keywords and variables

Keywords and variables	Description	Default	Availability
<code>dpd-idlecleanup</code> <seconds_integer>	The DPD long idle setting when <code>dpd</code> is set to <code>enable</code> . Set the time, in seconds, that a link must remain unused before the local VPN peer pro-actively probes its state. After this period of time expires, the local peer will send a DPD probe to determine the status of the link even if there is no traffic between the local peer and the remote peer. The <code>dpd-idlecleanup</code> range is 100 to 28 800 and must be greater than the <code>dpd-idleworry</code> setting.	300 seconds	All models. dpd must be set to <code>enable</code> .
<code>dpd-idleworry</code> <seconds_integer>	The DPD short idle setting when <code>dpd</code> is set to <code>enable</code> . Set the time, in seconds, that a link must remain unused before the local VPN peer considers it to be idle. After this period of time expires, whenever the local peer sends traffic to the remote VPN peer it will also send a DPD probe to determine the status of the link. The <code>dpd-idleworry</code> range is 1 to 300.  To control the length of time that the FortiGate unit takes to detect a dead peer with DPD probes, use the <code>dpdretrycount</code> and <code>dpd-retryinterval</code> keywords.	10 seconds	All models. dpd must be set to <code>enable</code> .

**ipsec phase1 command keywords and variables (Continued)**

Keywords and variables	Description	Default	Availability
dpd-retrycount <retry_integer>	The DPD retry count when dpd is set to enable. Set the number of times that the local VPN peer sends a DPD probe before it considers the link to be dead and tears down the security association (SA). The dpd-retrycount range is 0 to 10. To avoid false negatives due to congestion or other transient failures, set the retry count to a sufficiently high value for your network.	3	All models. dpd must be set to enable.
dpd-retryinterval <seconds_integer>	The DPD retry interval when dpd is set to enable. Set the time, in seconds, that the local VPN peer waits between sending DPD probes. The dpd-retryinterval range is 1 to 60.	5 seconds	All models. dpd must be set to enable.

**Example**

Use the following command to edit an IPsec VPN phase 1 configuration with the following characteristics:

- Phase 1 configuration name: Simple\_GW
- Remote peer address type: Dynamic
- Encryption and authentication proposal: des-md5
- Authentication method: psk
- Pre-shared key: Qf2p3093jIj2bz7E
- Mode: aggressive
- Dead Peer Detection: enable
- Long idle: 1000
- Short idle: 150
- Retry count: 5
- Retry interval: 30

```

config vpn ipsec phase1
  edit Simple_GW
    set Type dynamic
    set proposal des-md5
    set authmethod psk
    set psksecret Qf2p3093jIj2bz7E
    set mode aggressive
    set dpd enable
    set dpd-idlecleanup 1000
    set dpd-idleworry 150
    set dpd-retrycount 5
    set dpd-retryinterval 30
  end

```

## ipsec phase2

Use the `config vpn ipsec phase2` CLI command to add or edit an IPSec VPN phase 2 configuration.

### Command syntax pattern

```
config vpn ipsec phase2
  edit <name_str>
    set <keyword> <variable>
  end

config vpn ipsec phase2
  edit <name_str>
    unset <keyword>
  end

config vpn ipsec phase2
  delete <name_str>
end

get vpn ipsec phase2 [<name_str>]

show vpn ipsec phase2 [<name_str>]
```

### ipsec phase2 command keywords and variables

Keywords and variables	Description	Default	Availability
<code>bindtoif</code> <interface-name_str>	Bind the tunnel to the specified network interface. Type the name of the local FortiGate interface.	No default.	All models.
<code>dstaddr</code> <name_str>	Enter the name of the firewall destination IP address that corresponds to the recipient or network behind the remote VPN peer. You must create the firewall address before you can select it here. For more information, see <a href="#">“Adding firewall policies for IPSec VPN tunnels”</a> on page 266.	No default.	All models. selector must be set to specify.
<code>dstport</code> <port_integer>	Enter the port number that the remote VPN peer uses to transport traffic related to the specified service (see <code>protocol</code> ). The <code>dstport</code> range is 1 to 65535. To specify all ports, type 0.	No default.	All models. selector must be set to specify.
<code>protocol</code> <protocol_integer>	Enter the IP protocol number for the service. The <code>protocol</code> range is 1 to 255. To specify all services, type 0.	No default.	All models. selector must be set to specify.

**ipsec phase2 command keywords and variables (Continued)**

Keywords and variables	Description	Default	Availability
<code>selector { policy   wildcard   specify}</code>	Enter the method for choosing selectors for IKE negotiations: <ul style="list-style-type: none"> <li>• Select <code>policy</code> to choose a selector from a firewall encryption policy. The VPN tunnel referenced in the firewall encryption policy will be referenced.</li> <li>• Select <code>wildcard</code> to disable selector negotiation for this tunnel. Use this option to avoid negotiation errors (such as invalid ID Information) that may occur during quick mode when the set of policies between the peers is not symmetric.</li> <li>• Select <code>specify</code> to specify the firewall encryption policy source and destination IP addresses, ports, and IP protocol to use for selector negotiation. When you choose <code>specify</code>, you must also enter values for the <code>srcaddr</code>, <code>dstaddr</code>, <code>protocol</code>, <code>srcport</code>, and <code>dstport</code> keywords.</li> </ul>	<code>policy</code>	All models.
<code>single-source {disable   enable}</code>	Enable or disable all dialup clients to connect using the same phase 2 tunnel definition.	<code>disable</code>	All models.
<code>srcaddr &lt;name_str&gt;</code>	Enter the name of the firewall source IP address that corresponds to the local sender or network behind the local VPN peer. You must create the firewall address before you can select it here. For more information, see <a href="#">“Adding firewall policies for IPSec VPN tunnels” on page 266</a> .	No default.	All models. <code>selector</code> must be set to <code>specify</code> .
<code>srcport &lt;port_integer&gt;</code>	Enter the port number that the local VPN peer uses to transport traffic related to the specified service (see <code>protocol</code> ). The <code>srcport</code> range is 1 to 65535. To specify all ports, type 0.	No default.	All models. <code>selector</code> must be set to <code>specify</code> .

**ipsec vip**

A FortiGate unit can act as a proxy by answering ARP requests locally and forwarding the associated traffic to the intended destination host over an IPSec VPN tunnel. The feature is intended to enable IPSec VPN communications between two hosts that coordinate the same private address space on physically separate networks. The IP addresses of both the source host and the destination host must be unique. The `ipsec vip` command lets you specify the IP addresses that can be accessed at the remote end of the VPN tunnel. You must configure IPSec virtual IP (VIP) addresses at both ends of the IPSec VPN tunnel.

Adding an IPSec VIP entry to the VIP table enables a FortiGate unit to respond to ARP requests destined for remote servers and route traffic to the intended destinations automatically. Each IPSec VIP entry is identified by an integer. An entry identifies the name of the FortiGate interface to the destination network, and the IP address of a destination host on the destination network. Specify an IP address for every host that needs to be accessed on the other side of the tunnel—you can define a maximum of 32 IPSec VIP addresses on the same interface.





**Note:** The interface to the destination network must be associated with a VPN tunnel through a firewall encryption policy (`action` must be set to `encrypt`). The policy determines which VPN tunnel will be selected to forward traffic to the destination. When you create IPsec VIP entries, check the encryption policy on the FortiGate interface to the destination network to ensure that it meets your requirements.

For more information, see [“Configuring IPsec virtual IP addresses” on page 274](#).

## Command syntax pattern

```
config vpn ipsec vip
  edit <vip_integer>
    set <keyword> <variable>
  end

config vpn ipsec vip
  edit <vip_integer>
    unset <keyword>
  end

config vpn ipsec vip
  delete <vip_integer>
end

get vpn ipsec vip [<vip_integer>]

show vpn ipsec vip [<vip_integer>]
```

## ipsec vip command keywords and variables

Keywords and variables	Description	Default	Availability
ip <address_ipv4>	The IP address of the destination host on the destination network.	0.0.0.0	All models.
out-interface <interface-name_str>	The name of the FortiGate interface to the destination network.	null	All models.

## Example

The following commands add IPsec VIP entries for two remote hosts that can be accessed by a FortiGate unit through an IPsec VPN tunnel on the `external` interface of the FortiGate unit. Similar commands must be entered on the FortiGate unit at the other end of the IPsec VPN tunnel.

```
config vpn ipsec vip
  edit 1
    set ip 192.168.12.1
    set out-interface external
  next
  edit 2
    set ip 192.168.12.2
    set out-interface external
end
```



**Note:** Typing `next` lets you define another VIP address without leaving the `vip` shell.

This example shows how to display the settings for the `vpn ipsec vip` command.

```
get vpn ipsec vip
```

This example shows how to display the settings for the VIP entry named 1.

```
get vpn ipsec vip 1
```

This example shows how to display the current configuration of all existing VIP entries.

```
show vpn ipsec vip
```

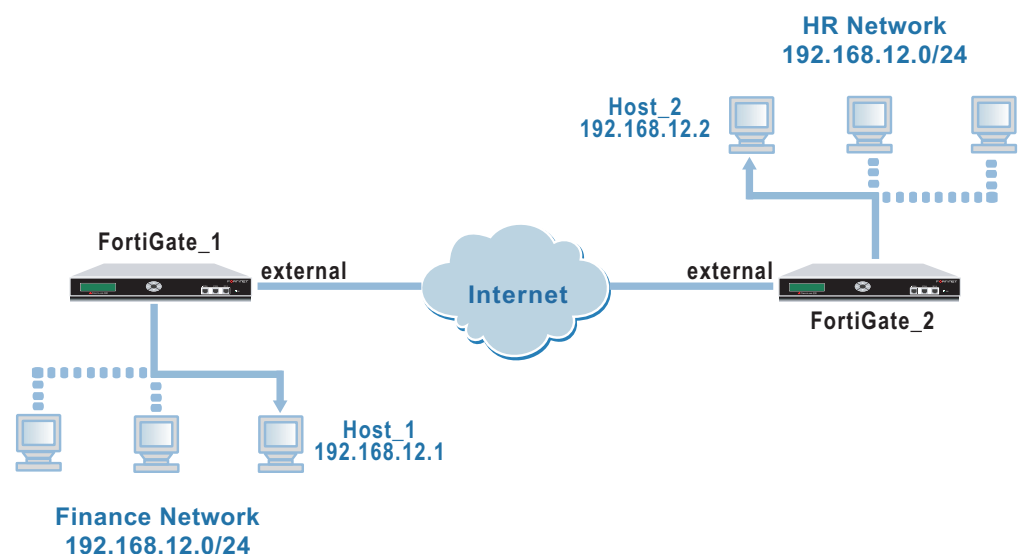
## Configuring IPsec virtual IP addresses

Use the FortiGate unit's IPsec VIP feature to enable hosts on physically different networks to communicate with each other as if they were connected to the same private network. This feature can be configured manually through CLI commands.

When the destination IP address in a local ARP request matches an entry in the FortiGate unit's virtual IP (VIP) table, the FortiGate unit responds with its own MAC address and forwards traffic to the correct destination at the other end of the VPN tunnel afterward.

Consider the following example, which shows two physically separate networks. The IP addresses of the computers on both networks are in the 192.168.12.0/24 range, but no two IP addresses are the same. An IPsec VPN has been configured between FortiGate\_1 and FortiGate\_2. The FortiGate configuration permits Host\_1 on the Finance network to transmit data to Host\_2 on the HR network through the IPsec VPN tunnel.

**Figure 141:** A typical site-to-site configuration using the IPsec VIP feature



When Host\_1 attempts to send a packet to Host\_2 for the first time, Host\_1 issues an ARP request locally for the MAC address of Host\_2. However, because Host\_2 resides on a remote network, it does not respond. Instead, the FortiGate unit responds with its own MAC address. From that point, Host\_1 adds the MAC address of the FortiGate unit to its ARP cache and the FortiGate unit will act as a proxy for Host\_2.

In the above example, the private IP addresses between the two sites have been coordinated to protect against ambiguous routing (no two IP addresses are the same).

Setting up a configuration like this involves performing the following tasks at FortiGate\_1 and FortiGate\_2.

To enable IPsec VPN communication between two network hosts that coordinate the same private address space on physically separate networks, perform the following tasks at the local and remote FortiGate units:

- 1 On both FortiGate units, define the gateway/tunnel on which to transmit VPN traffic to the remote location (see [“Phase 1” on page 246](#) and [“Phase 2” on page 250](#)).
- 2 On both FortiGate units, define the firewall encrypt policy that is needed to select and enable communication through the defined VPN gateway/tunnel (see [“Adding firewall policies for IPsec VPN tunnels” on page 266](#)).
- 3 Using CLI commands to configure the local FortiGate unit, add VIP entries to define which IP addresses can be accessed at the remote end of the VPN tunnel (see [“ipsec vip” on page 272](#)). For example, to enable access to Host\_2 on the HR network from Host\_1 on the Finance network, enter the following CLI commands on FortiGate\_1:

```
config vpn ipsec vip
edit 1
    set ip 192.168.12.2
    set out-interface external
end
```

- 4 Using CLI commands to configure the remote FortiGate unit, add VIP entries to define which IP addresses can be accessed at the local end of the VPN tunnel (see [“ipsec vip” on page 272](#)). For example, to enable access to Host\_1 on the Finance network from Host\_2 on the HR network, enter the following CLI commands on FortiGate\_2:

```
config vpn ipsec vip
edit 1
    set ip 192.168.12.1
    set out-interface external
end
```



# IPS

The FortiGate Intrusion Prevention System (IPS) combines signature- and anomaly-based intrusion detection and prevention with low latency and excellent reliability. The FortiGate unit can record suspicious traffic in logs, can send alert email to system administrators, and can log, pass, drop, reset, or clear suspicious packets or sessions. You can adjust some IPS anomaly thresholds to work best with the normal traffic on the protected networks. You can also create custom signatures to customize the FortiGate IPS for diverse network environments.

You can configure the IPS globally and then enable or disable all signatures or all anomalies in individual firewall protection profiles. [Table 23](#) describes the IPS settings and where to configure and access them. To access protection profile IPS options go to Firewall > Protection Profile, select edit or Create New, and select IPS. See [“Protection profile options” on page 223](#).

**Table 23: IPS and Protection Profile IPS configuration**

Protection Profile IPS options	IPS setting
IPS Signature	IPS > Signature
Enable or disable IPS signatures for all network services.	View and configure a list of predefined signatures. Create custom signatures based on the network requirements.
IPS Anomaly	IPS > Anomaly
Enable or disable IPS anomalies for all network services.	View and configure a list of predefined anomalies.

## Protection profile configuration

For information about adding protection profiles to firewall policies, see [“To add a protection profile to a policy” on page 229](#).

## IPS updates and information

FortiProtect services are a valuable customer resource and include automatic updates of virus and IPS (attack) engines and definitions through the FortiProtect Distribution Network (FDN). The FortiProtect Center also provides the FortiProtect virus and attack encyclopedia and the FortiProtect Bulletin.

Visit the FortiProtect Center at <http://www.fortinet.com/FortiProtectCenter/>.

To set up automatic and push updates see [“Update center” on page 118](#).

This chapter describes:

- [Signature](#)
- [Anomaly](#)
- [Configuring IPS logging and alert email](#)
- [Default fail open setting](#)

## Signature

The FortiGate IPS matches network traffic against patterns contained in attack signatures. Attack signatures reliably protect your network from known attacks. Fortinet's FortiProtect infrastructure ensures the rapid identification of new threats and the development of new attack signatures.

You can configure the FortiGate unit to automatically check for and download an updated attack definition file containing the latest signatures, or you can manually download the updated attack definition file. You can also configure the FortiGate unit to allow push updates of updated attack definition files as soon as they are available from the FortiProtect Distribution Network. For details, see ["Update center" on page 118](#).

When the FortiGate unit installs an updated attack definition file, it checks to see if the default configuration for any existing signatures has changed. If the default configuration has changed, the changes are preserved.

In addition to an extensive list of predefined attack signatures, you can also create your own custom attack signatures for the FortiGate unit. See ["Adding custom signatures" on page 283](#).

### Predefined

Predefined signatures are arranged into groups based on the type of attack. By default, all signature groups are enabled while some signatures within groups are not. Check the default settings to ensure they meet the requirements of your network traffic.

You can enable or disable signature groups or individual signatures. Disabling unneeded signatures can improve system performance and reduce the number of log messages and alert emails that the IPS generates. For example, the IPS detects a large number of web server attacks. If you do not provide access to a web server behind your FortiGate unit, you can disable all web server attack signatures.

Some signature groups include configurable parameters. The parameters that are available depend on the type of signatures in the signature group. When you configure these parameters for a signature group, the parameters apply to all of the signatures in the group.

For each signature, you can configure the action the FortiGate IPS takes when it detects an attack. The FortiGate IPS can pass, drop, reset or clear packets or sessions.

You can also enable or disable logging of the attack.

## Predefined signature list

You can enable or disable groups of predefined signatures and configure the settings for individual predefined signatures from the predefined signature list.

**Figure 142:**A portion of the predefined signature list

Name	Enable	Logging	Action	Revision	Modify
▶ apache					
▶ backdoor					
▶ cgi					
▶ coldfusion					
▼ compromise					
OpenSSH.GOBBLER.E			Pass	2.135	
OpenSSH.GOBBLER.Response.*GOBBLE*			Reset Client	2.135	
OpenSSH.GOBBLER.Response.Username			Pass	2.135	
▶ ddos					
▶ dns					
▶ dos					
▶ exploit					

<b>Group Name</b>	The signature group names.
<b>Enable</b>	The status of the signature group. A white check mark in a green circle indicates the signature group is enabled. A white X in a grey circle indicates the signature group is disabled.
<b>Logging</b>	The logging status for individual signatures. Click on the blue triangle to show the signature group members. A white check mark in a green circle indicates logging is enabled for the signature. A white X in a grey circle indicates logging is disabled for the signature.
<b>Action</b>	The action set for individual signatures. Click on the blue triangle to show the signature group members. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session. See <a href="#">Table 24</a> .
<b>Revision</b>	The revision number for individual signatures. To show the signature group members, click on the blue triangle.
<b>Modify</b>	The Configure and Reset icons. Reset only appears when the default settings have been modified. Selecting Reset restores the default settings.

[Table 24](#) describes each possible action you can select for predefined signatures.

**Table 24:** Actions to select for each predefined signature

Action	Description
Pass	The FortiGate unit lets the packet that triggered the signature pass through the firewall. If logging is disabled and action is set to Pass, the signature is effectively disabled.
Drop	The FortiGate unit drops the packet that triggered the signature. Fortinet recommends using an action other than Drop for TCP connection based attacks.
Reset	The FortiGate unit drops the packet that triggered the signature, sends a reset to both the client and the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established it acts as Clear Session.

**Table 24: Actions to select for each predefined signature**

Reset Client	The FortiGate unit drops the packet that triggered the signature, sends a reset to the client, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established it acts as Clear Session.
Reset Server	The FortiGate unit drops the packet that triggered the signature, sends a reset to the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established it acts as Clear Session.
Drop Session	The FortiGate unit drops the packet that triggered the signature and drops any other packets in the same session.
Clear Session	The FortiGate unit drops the packet that triggered the signature, removes the session from the FortiGate session table, and does not send a reset.
Pass Session	The FortiGate unit lets the packet that triggered the signature and all other packets in the session pass through the firewall.

## Configuring predefined signatures

### To enable or disable predefined signature groups

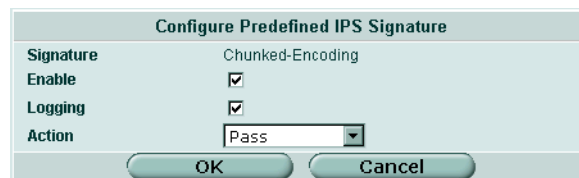
- 1 Go to **IPS > Signature > Predefined**.
- 2 Select the Configure icon next to the predefined signature group that you want to enable or disable.

**Figure 143: Enabling or disabling a predefined signature group**

- 3 Select the enable box to enable the predefined signature group or clear the enable box to disable the predefined signature group.
- 4 Select OK.

### To configure predefined signature settings

- 1 Go to **IPS > Signature > Predefined**.
- 2 Select the blue triangle next to a signature group name to display the members of that group.
- 3 Select the Configure icon for the signature you want to configure.

**Figure 144: Configuring predefined IPS signatures**



- 4 Select the Enable box to enable the signature or clear the Enable box to disable the signature.
- 5 Select the Logging box to enable logging for this signature or clear the Logging box to disable logging for this signature.
- 6 Select the Action for the FortiGate unit to take when traffic matches this signature. (See [Table 24.](#))
- 7 Select OK.

**To restore the recommended settings of a signature**

- 1 Go to **IPS > Signature > Predefined.**
- 2 Select the blue triangle next to a signature group name to display the members of that group.
- 3 Select the Reset icon for the signature you want to restore to recommended settings. The Reset icon is displayed only if the settings for the signature have been changed from recommended settings.
- 4 Select OK.

**Configuring parameters for dissector signatures**

The following predefined dissector signatures have configurable parameters.

- http\_decoder
- im
- p2p
- rpc\_decoder
- tcp\_reassembler

**Figure 145: Example of dissector signature parameters: tcp\_reassembler**

Edit IPS Configuration	
Group Name	tcp_reassembler
Enable	<input checked="" type="checkbox"/>
idle_timeout	120
min_ttl	2
port_list	21, 23, 25, 53, 80, 110, 111, 1
bad_flag_list	NULL, F, U, P, SF, PF, UP, UPF, I
direction	from-client
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Figure 146: Example of dissector signature parameters: p2p**

Configure Predefined IPS Signature	
Signature	kazaa
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Pass
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

<b>idle_timeout</b>	If a session is idle for longer than this number of seconds, the session will not be maintained by tcp_reassembler.
<b>min_ttl</b>	A packet with a higher ttl number in its IP header than the number specified here is not processed by tcp_reassembler.
<b>port_list</b>	A comma separated list of ports. The dissector can decode these TCP ports.
<b>bad_flag_list</b>	A comma separated list of bad TCP flags.
<b>reassembly_direction</b>	Valid settings are from-server, from-client, or both.
<b>codepoint</b>	A number from 0 to 63. Used for differentiated services tagging. When the action for p2p and im signatures is set to Pass, the FortiGate unit checks the codepoint. If the codepoint is set to a number from 1 to 63, the codepoint for the session is changed to the specified value. If the codepoint is set to -1 (the default) no change is made to the codepoint in the IP header.

## Custom

You can create custom IPS signatures. The custom signatures you create are added to a single Custom signature group.

Custom signatures provide the power and flexibility to customize the FortiGate IPS for diverse network environments. The FortiGate predefined signatures cover common attacks. If you are using an unusual or specialized application or an uncommon platform, you can add custom signatures based on the security alerts released by the application and platform vendors.

You can also use custom signatures to block or allow specific traffic. For example to block traffic containing pornography, you can add custom signatures similar to the following:

```
F-SBID (--protocol tcp; --flow established; --content "nude cheerleader"; --no_case)
```

When you add the signature set action to Drop Session.

For more information on custom signature syntax see the *FortiGate IPS Custom Signatures Technical Bulletin*.



**Note:** Custom signatures are an advanced feature. This document assumes the user has previous experience creating intrusion detection signatures.

## Custom signature list

Figure 147: The custom signature group

<input checked="" type="checkbox"/> Enable custom signature.						
<a href="#">Create New</a>						
Name	Revision	<input checked="" type="checkbox"/> Enable	Logging	Action	Modify	
ICMP10	2	<input checked="" type="checkbox"/>		Pass		

**Enable custom signature** Select the Enable custom signature box to enable the custom signature group or clear the Enable custom signature box to disable the custom signature group.

**Create New** Select Create New to create a new custom signature.

<b>Clear all custom signatures</b>	Remove all the custom signatures from the custom signature group.
<b>Reset to recommended settings?</b>	Reset all the custom signatures to the recommended settings.
<b>Name</b>	The custom signature names.
<b>Revision</b>	The revision number for each custom signature. The revision number is a number you assign to the signature when you create or revise it.
<b>Enable</b>	The status of each custom signature. A white check mark in a green circle indicates the signature is enabled. A white X in a grey circle indicates the signature is disabled. Selecting the box at the top of the Enable column enables all the custom signatures. Clearing the box at the top of the Enable column disables all the custom signatures.
<b>Logging</b>	The logging status of each custom signature. A white check mark in a green circle indicates logging is enabled for the custom signature. A white X in a grey circle indicates logging is disabled for the custom signature.
<b>Action</b>	The action set for each custom signature. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session.
<b>Modify</b>	The Delete and Edit/View icons.

## Adding custom signatures

### To add a custom signature

- 1 Go to **IPS > Signature > Custom**.
- 2 Select Create New to add a new custom signature or select the Edit icon to edit an existing custom signature.

**Figure 148:Edit custom signature**

- 3 Enter a name for the custom signature.  
You cannot edit the name of an existing custom signature.
- 4 Enter the custom signature.
- 5 Select the action to be taken when a packet triggers this signature. (See [Table 24](#) for action descriptions.)
- 6 Select the Logging box to enable logging for the custom signature or clear the Logging box to disable logging for the custom signature.

## Backing up and restoring custom signature files

For information on backing up and restoring the custom signature list, see [“Backing up and Restoring” on page 116](#).



**Caution:** Restoring the custom signature list overwrites the existing file.

## Anomaly

The FortiGate IPS uses anomaly detection to identify network traffic that does not fit known or preset traffic patterns. The FortiGate IPS identifies the four statistical anomaly types for the TCP, UDP, and ICMP protocols.

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

You can enable or disable logging for each anomaly, and you can control the IPS action in response to detecting an anomaly. In many cases you can also configure the thresholds that the anomaly uses to detect traffic patterns that could represent an attack.



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

You can also use the command line interface (CLI) to configure session control based on source and destination network address. See [“Anomaly CLI configuration” on page 287](#).

The anomaly detection list can be updated only when the FortiGate firmware image is upgraded.

### Anomaly list

**Figure 149:**The Anomaly list

Name	Enable	Logging	Action	Modify
syn_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Clear Session	
portscan	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Clear Session	
syn_fin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Clear Session	

**Name** The anomaly names.

**Enable** The status of the anomaly. A white check mark in a green circle indicates the anomaly is enabled. A white X in a grey circle indicates the anomaly is disabled.

**Logging** The logging status for each anomaly. A white check mark in a green circle indicates logging is enabled for the anomaly. A white X in a grey circle indicates logging is disabled for the anomaly.

- Action** The action set for each anomaly. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session.
- Modify** The Edit and Reset icons. If you have changed the settings for an anomaly, you can use the Reset icon to change the settings back to the recommended settings.

### Configuring an anomaly

Each anomaly is preset with a recommended configuration. By default all anomaly signatures are enabled. You can use the recommended configurations or you can modify the recommended configurations to meet the needs of your network.

For more information on minimum, maximum, and recommended thresholds for the anomalies with configurable thresholds, see the *FortiGate IPS Anomaly Thresholds and Dissector Values Technical Bulletin*.

**Figure 150:Editing the portscan IPS anomaly**

Edit IPS Anomaly	
Name	portscan
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Drop
Parameters:	
threshold	1000
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Figure 151:Editing the syn\_fin IPS anomaly**

Edit IPS Anomaly	
Name	syn_fin
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Clear Session
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- Name** The anomaly name.
- Enable** Select the Enable box to enable the anomaly or clear the Enable box to disable the anomaly.
- Logging** Select the Logging box to enable logging for the anomaly or clear the Logging box to disable logging for the anomaly.
- Action** Select an action for the FortiGate unit to take when traffic triggers this anomaly.
  - Pass** The FortiGate unit lets the packet that triggered the anomaly pass through the firewall. If logging is disabled and action is set to Pass, the anomaly is effectively disabled.
  - Drop** The FortiGate unit drops the packet that triggered the anomaly. Fortinet recommends using an action other than Drop for TCP connection based attacks.

<b>Reset</b>	The FortiGate unit drops the packet that triggered the anomaly, sends a reset to both the client and the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established it acts as Clear Session.
<b>Reset Client</b>	The FortiGate unit drops the packet that triggered the anomaly, sends a reset to the client, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established it acts as Clear Session.
<b>Reset Server</b>	The FortiGate unit drops the packet that triggered the anomaly, sends a reset to the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established it acts as Clear Session.
<b>Drop Session</b>	The FortiGate unit drops the packet that triggered the anomaly and drops any other packets in the same session.
<b>Clear Session</b>	The FortiGate unit drops the packet that triggered the anomaly, removes the session from the FortiGate session table, and does not send a reset.
<b>Pass Session</b>	The FortiGate unit lets the packet that triggered the anomaly and all other packets in the session pass through the firewall.
<b>threshold</b>	Traffic over the specified threshold triggers the anomaly.

### To configure the settings of an anomaly

- 1 Go to **IPS > Anomaly**.
- 2 Select the Edit icon for the signature you want to configure.
- 3 Select the Enable box to enable the anomaly or clear the Enable box to disable the anomaly.
- 4 Select the Logging box to enable logging for this anomaly or clear the Logging box to disable logging for this anomaly.
- 5 Select an action for the FortiGate unit to take when traffic triggers this anomaly.
- 6 Enter a new threshold value if required.
- 7 Select OK.

### To restore the default settings of an anomaly

- 1 Go to **IPS > Anomaly**.
- 2 Select the Reset icon for the anomaly you want to restore to defaults.

The Reset icon is displayed only if the settings for the anomaly have been changed from defaults.

- 3 Select OK.

## Anomaly CLI configuration



**Note:** This guide only covers Command Line Interface (CLI) commands that are not represented in the web-based manager. For complete descriptions and examples of how to use CLI commands see the *FortiGate CLI Reference Guide*.

### (config ips anomaly) config limit



**Note:** This command has more keywords than are listed in this Guide. See the *FortiGate CLI Reference Guide* for a complete list of commands and keywords.

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

You cannot edit the `default` entry. Addresses are matched from more specific to more general. For example, if you define thresholds for `192.168.100.0/24` and `192.168.0.0/16`, the address with the 24 bit netmask will be matched first.

### Command syntax pattern

```
config limit
  edit <name_str>
    set <keyword> <variable>
  end

config limit
  edit <name_str>
    unset <keyword>
  end

config limit
  delete <name_str>
```

### limit command keywords and variables

Keywords and variables	Description	Default	Availability
<code>ipaddress</code> <code>&lt;address_ipv4mask&gt;</code>	The ip address and netmask of the source or destination network.	No default.	All models.
<code>threshold</code> <code>&lt;threshold_integer&gt;</code>	Set the threshold that triggers this anomaly.	No default.	All models.

### Example

Use the following command to configure the limit for the `tcp_src_session` anomaly.

```
config ips anomaly tcp_src_session
  config limit
    edit subnet1
      set ipaddress 1.1.1.0 255.255.255.0
      set threshold 300
    end
  end
```

## Configuring IPS logging and alert email

Whenever the IPS detects or prevents an attack, it generates an attack message. You can configure the FortiGate unit to add the message to the attack log and to send an alert email to administrators. You can configure how often the FortiGate unit sends alert email. You can also reduce the number of log messages and alerts by disabling signatures for attacks that your system is not vulnerable to (for example, web attacks when you are not running a web server). For more information on FortiGate logging and alert email, see [“Log & Report” on page 339](#).

## Default fail open setting

If for any reason the IPS should cease to function, it will fail open by default. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved.

You can change the default fail open setting using the CLI:

```
config sys global
    set ips-open [enable | disable]
end
```

Enable `ips_open` to cause the IPS to fail open and disable `ips_open` to cause the IPS to fail closed.



# Antivirus

Antivirus provides configuration access to most of the antivirus options you enable when you create a firewall protection profile. While antivirus settings are configured for system-wide use, you can implement specific settings on a per profile basis.

[Table 25](#) describes the antivirus settings and where to configure and access them. To access protection profile antivirus options go to Firewall > Protection Profile, select edit or Create New, and select Anti-Virus. See [“Protection profile options” on page 223](#).

**Table 25: Antivirus and Protection Profile antivirus configuration**

Protection Profile antivirus options	Antivirus setting
Virus Scan	Antivirus > Config > Virus List
Enable or disable virus scanning for each protocol (HTTP, FTP, IMAP, POP3, SMTP).	View a read-only list of current viruses.
File Block	Antivirus > File Block
Enable or disable file blocking for each protocol.	Configure file patterns to block, enable or disable blocking for each protocol.
Quarantine	Antivirus > Quarantine
Enable or disable quarantining for each protocol. Quarantine is only available on units with a local disk.	View and sort the list of quarantined files, configure file patterns to upload automatically to Fortinet for analysis, and configure quarantining options in AntiVirus.
Pass fragmented emails	
Enable or disable passing fragmented emails. Fragmented emails cannot be scanned for viruses.	
Oversized file/email	Antivirus > Config > Config
Configure the FortiGate unit to block or pass oversized files and emails for each protocol.	Set the size thresholds for files and emails for each protocol in Antivirus. Go to Antivirus > Config > Grayware to enable blocking grayware programs.
Add signature to outgoing emails	
Create and enable a signature to append to outgoing emails (SMTP only).	

## Protection profile configuration

For information about configuring Protection Profiles, see “[Protection profile](#)” on [page 222](#). For information about adding protection profiles to firewall policies, see “[To add a protection profile to a policy](#)” on [page 229](#).

## Order of antivirus operations

Antivirus processing includes various modules and engines that perform separate tasks. The FortiGate unit performs antivirus processing in the order the features appear in the web-based manager menu: file block, virus scan, and grayware, followed by heuristics, which is configurable only through the CLI.

## Virus list updates and information

FortiProtect services are an excellent resource and include automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam RBL, through the FortiProtect Distribution Network (FDN). The FortiProtect Center also provides the FortiProtect virus and attack encyclopedia and the FortiProtect Bulletin.

Visit the FortiProtect Center at <http://www.fortinet.com/FortiProtectCenter/>.

To set up automatic and push updates see “[Update center](#)” on [page 118](#).

This chapter describes:

- [File block](#)
- [Quarantine](#)
- [Config](#)
- [CLI configuration](#)

# File block

Configure file blocking to remove all files that are a potential threat and to prevent active computer virus attacks. You can block files by name, by extension, or any other pattern, giving you the flexibility to block potentially harmful content.



**Note:** File block entries are not case sensitive. For example, adding \* .exe to the file block list also blocks any files ending in .EXE.

For standard operation, you can choose to disable file blocking in the Protection Profile, and enable it only to temporarily block specific threats as they occur. You can also enable or disable file blocking by protocol for each file pattern you configure.

The FortiGate unit blocks files that match a configured file pattern and displays a replacement message instead. The FortiGate unit also writes a message to the virus log and sends an alert email if configured to do so.

If both file block and virus scan are enabled, the FortiGate unit blocks files that match enabled file patterns and does not scan these files for viruses.

This section describes:

- [File block list](#)
- [Configuring the file block list](#)

## File block list

The file block list is preconfigured with a default list of file patterns:

- executable files (\*.bat, \*.com, and \*.exe)
- compressed or archive files (\*.gz, \*.rar, \*.tar, \*.tgz, and \*.zip)
- dynamic link libraries (\*.dll)
- HTML application (\*.hta)
- Microsoft Office files (\*.doc, \*.ppt, \*.xl?)
- Microsoft Works files (\*.wps)
- Visual Basic files (\*.vb?)
- screen saver files (\*.scr)
- program information files (\*.pif)

**Figure 152:Default file block list**

Pattern	Check All	<input type="checkbox"/> HTTP	<input type="checkbox"/> FTP	<input type="checkbox"/> IMAP	<input type="checkbox"/> POP3	<input type="checkbox"/> SMTP	
*.bat	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.com	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.dll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.doc	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.exe	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.gz	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.hta	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.ppt	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.rar	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.scr	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.tar	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.tgz	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.vb?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.wps	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.xl?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.zip	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
*.pif	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

File block list has the following icons and features:

<b>Create New</b>	Select Create New to add a new file pattern to the file block list.
<b>Apply</b>	Select Apply to apply any changes to the file block configuration.
<b>Pattern</b>	The current list of blocked file patterns. You can create a pattern by using ? or * wildcard characters.
<b>Check All</b>	Select a check box beside a file pattern to enable blocking that pattern for all types of traffic. Select a check box beside a service (HTTP, FTP, IMAP, POP3, and SMTP) to enable blocking all file patterns for that service.
<b>HTTP</b>	Displays a check mark if file blocking is enabled to block the file pattern in HTTP traffic.

<b>FTP</b>	Displays a check mark if file blocking is enabled to block the file pattern in FTP traffic.
<b>IMAP</b>	Displays a check mark if file blocking is enabled to block the file pattern in IMAP traffic.
<b>POP3</b>	Displays a check mark if file blocking is enabled to block the file pattern in POP3 traffic.
<b>SMTP</b>	Displays a check mark if file blocking is enabled to block the file pattern in SMTP traffic.

The Delete and Edit/View icons.

## Configuring the file block list

### To add a file name or file pattern to the file block list

- 1 Go to **Anti-Virus > File Block**.
- 2 Enter the file name or file pattern you want to add.
- 3 Select Create New.
- 4 Select the protocols for which you want to block the file, or select Check All.
- 5 Select Apply.

## Quarantine

FortiGate units with a local disk can quarantine blocked and infected files. You can view the file names and status information about the file in the quarantined file list. You can also submit specific files and add file patterns to the AutoSubmit list so they will automatically be uploaded to FortiNet for analysis.













This section describes:

- [Quarantined files list](#)
- [Quarantined files list options](#)
- [AutoSubmit list](#)
- [AutoSubmit list options](#)
- [Configuring the AutoSubmit list](#)
- [Config](#)

### Quarantined files list

The quarantined files list displays information about each file that is quarantined because of virus infection or file blocking. You can sort the files by any one of file name, date, service, status, duplicate count (DC), or time to live (TTL). You can also filter the list to view only quarantined files with a specific status or from a specific service.

Figure 153: Sample quarantined files list

File Name	Date	Service	Status	Status Description	DC	TTL	Upload Status	
winx331.exe	03/15/2004 20:53	POP3	Blocked	File was stopped by file block pattern.	0	EXP.	N	  
AUTOPLAY.EXE	03/15/2004 20:54	POP3	Blocked	File was stopped by file block pattern.	0	EXP.	N	  
AFWeeklyReport.doc	03/15/2004 20:46	POP3	Blocked	File was stopped by file block pattern.	1	EXP.	N	  
Internet.doc	03/15/2004 20:53	POP3	Blocked	File was stopped by file block pattern.	0	EXP.	Y	  

## Quarantined files list options

The quarantined files list has the following features and displays the following information about each quarantined file:

<b>Apply</b>	Select Apply to apply the sorting and filtering selections to the quarantined files list.
<b>Sort by:</b>	Sort the list. Choose from: status, service, file name, date, TTL, or duplicate count. Click apply to complete the sort.
<b>Filter:</b>	Filter the list. Choose from status (infected, blocked, or heuristics) or service (IMAP, POP3, SMTP, FTP, or HTTP). Click apply to complete the filtering. Heuristics mode is configurable through the CLI only. See <a href="#">“CLI configuration” on page 299</a> .
<b>File Name</b>	The processed file name of the quarantined file. When a file is quarantined, all spaces are removed from the file name, and a 32-bit checksum is performed on the file. The file is stored on the FortiGate hard disk with the following naming convention: <32bit CRC>.<processed filename> For example, a file named Over Size.exe is stored as 3fc155d2.oversize.exe.
<b>Date</b>	The date and time that the file was quarantined, in the format dd/mm/yyyy hh:mm. This value indicates the time that the first file was quarantined if the duplicate count increases.
<b>Service</b>	The service from which the file was quarantined (HTTP, FTP, IMAP, POP3, SMTP).
<b>Status</b>	The reason the file was quarantined: infected, heuristics, or blocked.
<b>Status Description</b>	Specific information related to the status, for example, “File is infected with “W32/Klez.h”” or “File was stopped by file block pattern.”
<b>DC</b>	Duplicate count. A count of how many duplicates of the same file were quarantined. A rapidly increasing number can indicate a virus outbreak.
<b>TTL</b>	Time to live in the format hh:mm. When the TTL elapses, the FortiGate unit labels the file as EXP under the TTL heading. In the case of duplicate files, each duplicate found refreshes the TTL.
<b>Upload status</b>	Y indicates the file has been uploaded to Fortinet for analysis, N indicates the file has not been uploaded.  The Delete icon.  The Download icon. Download the corresponding file in its original format.  The Submit icon. Upload a suspicious file to Fortinet for analysis.



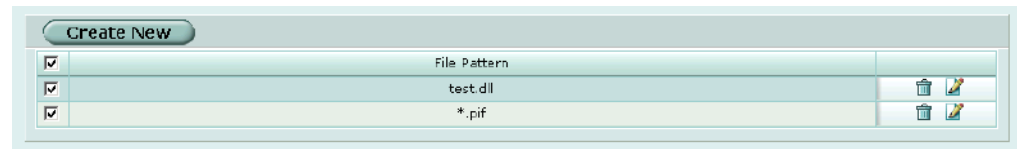
**Note:** Duplicates of files (based on the checksum) are not stored, only counted. The TTL value and the duplicate count are updated each time a duplicate of a file is found.

## AutoSubmit list

You can configure the FortiGate unit to automatically upload suspicious files to Fortinet for analysis. You can add file patterns to the AutoSubmit list using wildcard characters (\* or ?). File patterns are applied for AutoSubmit regardless of file blocking settings.

You can also upload files to Fortinet based on status (blocked or heuristics) or submit individual files directly from the quarantined files list. The FortiGate unit uses encrypted email to autosubmit files to an SMTP server through port 25.

**Figure 154: Sample AutoSubmit list**



## AutoSubmit list options

AutoSubmit list has the following icons and features:

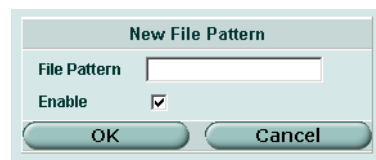
- Create New** Select Create New to add a new file pattern to the AutoSubmit list.
- File Pattern** The current list of file patterns that will be automatically uploaded. You can create a pattern by using ? or \* wildcard characters. Enable the check box to enable all file patterns in the list.  
The Delete and Edit/View icons.

## Configuring the AutoSubmit list

### To add a file pattern to the AutoSubmit list

- 1 Go to **Anti-Virus > Quarantine > AutoSubmit**.
- 2 Select Create New.

**Figure 155: Adding a file pattern**



- 3 Enter the file pattern or file name you want to automatically upload to Fortinet for analysis.
- 4 Select Enable.
- 5 Select OK.

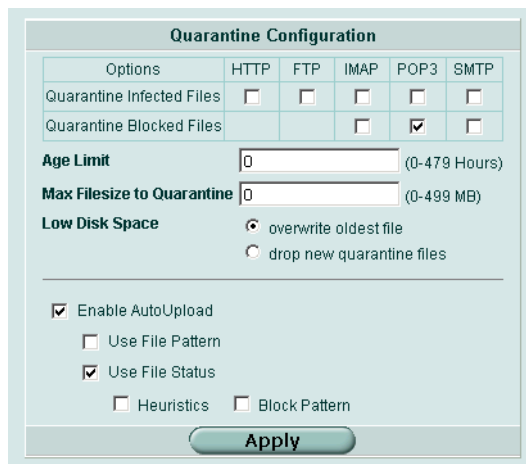


**Note:** To enable automatic uploading of the configured file patterns you must go to **Anti-Virus > Quarantine > Config**, select Enable AutoSubmit, and select Use File Pattern.

## Config

Go to Config to set quarantine configuration options including whether to quarantine blocked or infected files and from which service. You can also configure the time to live and file size values, and enable AutoSubmit settings.

**Figure 156: Quarantine configuration**



Quarantine configuration has the following options:

- Options**

Quarantine Infected Files: Select the protocols from which to quarantine infected files identified by antivirus scanning.

Quarantine Suspicious Files: Select the protocols from which to quarantine suspicious files identified by heuristics.

Quarantine Blocked Files. Select the protocols from which to quarantine blocked files identified by antivirus file blocking. The Quarantine Blocked Files option is not available for HTTP or FTP because a file name is blocked before downloading and cannot be quarantined.
- Age limit**

The time limit in hours for which to keep files in quarantine. The age limit is used to formulate the value in the TTL column of the quarantined files list. When the limit is reached the TTL column displays EXP. and the file is deleted (although a record is maintained in the quarantined files list). Entering an age limit of 0 (zero) means files are stored on disk indefinitely depending on low disk space action.
- Max filesize to quarantine**

The maximum size of quarantined files in MB. Setting the maximum file size too large may affect performance.
- Low disk space**

Select the action to take when the local disk is full: overwrite the oldest file or drop the newest file.
- Enable AutoSubmit**

Enable AutoSubmit: enables the AutoSubmit feature. Select one or both of the options below.

Use file pattern: Enables the automatic upload of files matching the file patterns in the AutoSubmit list.

Use file status: Enables the automatic upload of quarantined files based on their status. Select either heuristics or block pattern.

Heuristics is configurable through the CLI only. See [“CLI configuration” on page 299](#).
- Apply**

Select Apply to save the configuration.

## Config

Config displays a list of the current viruses blocked by the FortiGate unit. You can also configure file and email size limits, and grayware blocking.

This section describes:

- [Virus list](#)
- [Config](#)
- [Grayware](#)
- [Grayware options](#)

### Virus list

The virus list displays the current viruses blocked in alphabetical order. You can view the entire list or parts of the list by selecting the number or alphabet ranges. You can update this list manually or set up the FortiGate unit to receive automatic updates daily or whenever required. To manually upload a virus list update see [“Changing unit information” on page 29](#). To find out how to use the Fortinet Update Center, see [“Update center” on page 118](#).

**Figure 157:Virus list (partial)**

0 - 9 A - F G - L M - R S - Z All		
S-Bug.3471	S&F.2976	S&F.2976
Screaming_Fist	Satan_Family	Satan_Family
Shanghai_II.4077	Seventh_son.332.A	Seventh_son.332.A
SillyOE.100	SillyCR.122	SillyCR.122
Spanish_Foel.1417	Spam.Euthenesia	Spam.Euthenesia
Spanska.4250.A	Spanska.1500	Spanska.1500
Spy/Hiddukel	Spanska.4250.fam	Spanska.4250.fam
Stealth_Boot.C	Spybot.T-net	Spybot.T-net
Stoned.A	StealthBoot.C	StealthBoot.C
Stoned.Diablo	Stoned.DamsDoom	Stoned.DamsDoom
Stoned.Spirt	Stoned.No_INT.A	Stoned.No_INT.A
SubSeven.Backdoor	Stoned_Family	Stoned_Family

### Config

Oversize threshold configuration refers to the size limits you can apply to scan files and email in memory.

The maximum file size allowed in memory is usually 10% of the FortiGate RAM size. For example, a FortiGate unit with 256 MB of RAM could have a memory oversize threshold range of 1 to 25 MB. The range for each FortiGate unit is displayed in the web-based manager as shown in [Figure 158](#).



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



Figure 158: Example threshold configuration

Oversize Threshold Configuration		
Memory		
HTTP	<input type="text" value="10"/>	(1-139 MB)
FTP	<input type="text" value="10"/>	(1-139 MB)
IMAP	<input type="text" value="10"/>	(1-139 MB)
POP3	<input type="text" value="10"/>	(1-139 MB)
SMTP	<input type="text" value="10"/>	(1-139 MB)
<input type="button" value="Apply"/>		

You can enable oversized file blocking in a firewall protection profile. To access protection profiles go to Firewall > Protection Profile, select Anti-Virus > Oversized File/Email and choose to pass or block oversized email and files for each protocol.

Further file size limits for uncompressed files can be configured as an advanced feature via the CLI. See [“CLI configuration” on page 299](#).

## Grayware

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

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

## Grayware options

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

Figure 159: Sample grayware options

Category	Enable
▶ Adware	<input type="checkbox"/>
▶ Dial	<input type="checkbox"/>
Game	<input type="checkbox"/>
Joke	<input type="checkbox"/>
P2P	<input type="checkbox"/>
▶ Spy	<input type="checkbox"/>
Keylog	<input type="checkbox"/>
▶ Hijacker	<input type="checkbox"/>
▶ Plugin	<input type="checkbox"/>
NMT	<input type="checkbox"/>
RAT	<input type="checkbox"/>
Misc	<input type="checkbox"/>
BHD	<input type="checkbox"/>
Toolbar	<input type="checkbox"/>
Download	<input type="checkbox"/>

The categories may change or expand when the FortiGate unit receives updates. In the example above you can choose to enable the following grayware categories. Enabling a grayware category blocks all files listed in the category.

<b>Adware</b>	Select enable to block adware programs. Adware is usually embedded in freeware programs and causes ads to pop up whenever the program is opened or used.
<b>Dial</b>	Select enable to block dialer programs. Dialers allow others to use the PC modem to call premium numbers or make long distance calls.
<b>Game</b>	Select enable to block games. Games are usually joke or nuisance games that you may want to block from network users.
<b>Joke</b>	Select enable to block joke programs. Joke programs can include custom cursors and programs that appear to affect the system.
<b>P2P</b>	Select enable to block peer to peer communications programs. P2P, while a legitimate protocol, is synonymous with file sharing programs that are used to swap music, movies, and other files, often illegally.
<b>Spy</b>	Select enable to block spyware programs. Spyware, like adware, is often included with freeware. Spyware is a tracking and analysis program that can report your activities, such as web browsing habits, to the advertiser's web site where it may be recorded and analyzed.
<b>Keylog</b>	Select enable to block keylogger programs. Keylogger programs can record every keystroke made on a keyboard including passwords, chat, and instant messages.
<b>Hijacker</b>	Select enable to block browser hijacking programs. Browser hijacking occurs when a 'spyware' type program changes web browser settings, including favorites or bookmarks, start pages, and menu options.
<b>Plugin</b>	Select enable to block browser plugins. Browser plugins can often be harmless Internet browsing tools that are installed and operate directly from the browser window. Some toolbars and plugins can attempt to control or record and send browsing preferences.
<b>NMT</b>	Select enable to block network management tools. Network management tools can be installed and used maliciously to change settings and disrupt network security.
<b>RAT</b>	Select enable to block remote administration tools. Remote administration tools allow outside users to remotely change and monitor a computer on a network.
<b>Misc</b>	Select enable to block any programs included in the miscellaneous grayware category.
<b>BHO</b>	Select enable to block browser helper objects. BHOs are DLL files that are often installed as part of a software package so the software can control the behavior of Internet Explorer 4.x and higher. Not all BHOs are malicious, but the potential exists to track surfing habits and gather other information.
<b>Toolbar</b>	Select enable block custom toolbars. While some toolbars are harmless, spyware developers can use these toolbars to monitor web habits and send information back to the developer.
<b>Download</b>	Select enable to block download programs. Download components are usually run at Windows startup and are designed to install or download other software, especially advertising and dial software.

## CLI configuration



**Note:** This guide only covers Command Line Interface (CLI) commands that are not represented in the web-based manager. For complete descriptions and examples of how to use CLI commands see the *FortiGate CLI Reference Guide*.

### config antivirus heuristic

The FortiGate heuristic antivirus engine performs tests on files to detect virus-like behavior or known virus indicators. Heuristic scanning is performed last, after file blocking and virus scanning have found no matches. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results.

The heuristic engine is enabled by default to pass suspected files to the recipient and send a copy to quarantine. Once configured in the CLI, heuristic is enabled in a protection profile when Virus Scan is enabled.

Use the heuristic command to change the heuristic scanning mode.

### Command syntax pattern

```
config antivirus heuristic
    set <keyword> <variable>
end

config antivirus heuristic
    unset <keyword>
end

get antivirus heuristic

show antivirus heuristic
```

**Table 26: antivirus heuristic command keywords and variables**

Keywords and variables	Description	Default	Availability
mode {pass   block   disable}	Enter <code>pass</code> to enable heuristics but pass detected files to the recipient. Suspicious files are quarantined if quarantine is enabled. Enter <code>block</code> to enable heuristics and block detected files. A replacement message is forwarded to the recipient. Blocked files are quarantined if quarantine is enabled. Enter <code>disable</code> to disable heuristics.	pass	All models.

### Example

This example shows how to disable heuristic scanning.

```
config antivirus heuristic
    set mode disable
end
```

This example shows how to display the settings for the `antivirus heuristic` command.

```
get antivirus heuristic
```

This example shows how to display the configuration for the `antivirus heuristic` command.

```
show antivirus heuristic
```

## config antivirus quarantine

The quarantine command also allows configuration of heuristic related settings.



**Note:** This command has more keywords than are listed in this Guide. See the *FortiGate CLI Reference Guide* for a complete list of commands and keywords.

### Command syntax pattern

```
config antivirus quarantine
  set <keyword> <variable>
end

config antivirus quarantine
  unset <keyword>
end

get antivirus quarantine

show antivirus quarantine
```

### antivirus quarantine command keywords and variables

Keywords and variables	Description	Default	Availability
drop_heuristic {ftp http imap pop3 smtp}	Do not quarantine files found by heuristic scanning in traffic for the specified protocols.	imap smtp pop3 http ftp	FortiGate models numbered 200 and higher.
store_heuristic {ftp http imap pop3 smtp}	Quarantine files found by heuristic scanning in traffic for the specified protocols.	No default.	FortiGate models numbered 200 and higher.

## config antivirus service http

Use this command to configure how the FortiGate unit handles antivirus scanning of large files in HTTP traffic and what ports the FortiGate unit scans for HTTP.

### Command syntax pattern

```
config antivirus service http
  set <keyword> <variable>
end
```

```

config antivirus service http
    unset <keyword>
end

get antivirus service [http]

show antivirus service [http]

```

### antivirus service http command keywords and variables

Keywords and variables	Description	Default	Availability
memfilesizelimit <MB_integer>	Set the maximum file size (in megabytes) that can be buffered to memory for virus scanning. The maximum file size allowed is 10% of the FortiGate RAM size. For example, a FortiGate unit with 256 MB of RAM could have a threshold range of 1 MB to 25 MB. Note: For email scanning, the oversize threshold refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes less than the configured oversize threshold.	10 (MB)	All models.
port <port_integer>	Configure antivirus scanning on a nonstandard port number or multiple port numbers for HTTP. You can use ports from the range 1-65535. You can add up to 20 ports.	80	All models.
uncompsizelimit <MB_integer>	Set the maximum uncompressed file size that can be buffered to memory for virus scanning. Enter a value in megabytes between 1 and the total memory size. Enter 0 for no limit (not recommended).	10 (MB)	All models.

### How file size limits work

The `memfilesizelimit` is applied first to all incoming files, compressed or uncompressed. If the file is larger than the limit the file is passed or blocked according to the user configuration in the firewall profile.

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

## Example

This example shows how to set the maximum file size that can be buffered to memory for scanning at 12 MB, the maximum uncompressed file size that can be buffered to memory for scanning at 15 MB, and how to enable antivirus scanning on ports 70, 80, and 443 for HTTP traffic.

```
config antivirus service http
  set memfilesizelimit 12
  set uncompsizelimit 15
  set port 70
  set port 80
  set port 443
end
```

This example shows how to display the antivirus HTTP traffic settings.

```
get antivirus service http
```

This example shows how to display the configuration for antivirus HTTP traffic.

```
show antivirus service http
```

## config antivirus service ftp

Use this command to configure how the FortiGate unit handles antivirus scanning of large files in FTP traffic and how the FortiGate unit handles the buffering and uploading of files to an FTP server.

## Command syntax pattern

```
config antivirus service ftp
  set <keyword> <variable>
end

config antivirus service ftp
  unset <keyword>
end

get antivirus service [ftp]

show antivirus service [ftp]
```

## antivirus service ftp command keywords and variables

Keywords and variables	Description	Default	Availability
memfilesizelimit <MB_integer>	Set the maximum file size that can be buffered to memory for virus scanning. The maximum file size allowed is 10% of the FortiGate RAM size. For example, a FortiGate unit with 256 MB of RAM could have a threshold range of 1 MB to 25 MB. Oversized files can be passed or blocked in a firewall protection profile. Note: For email scanning, the memfilesizelimit refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes less than the memfilesizelimit.	10 (MB)	All models.
port <port_integer>	Configure antivirus scanning on a nonstandard port number or multiple port numbers for FTP. You can use ports from the range 1-65535. You can add up to 20 ports.	21	All models.
uncompsizelimit <MB_integer>	Set the maximum uncompressed file size that can be buffered to memory for virus scanning. Enter a value in megabytes between 1 and the total memory size. Enter 0 for no limit (not recommended).	10 (MB)	All models.

### How file size limits work

See [“How file size limits work”](#) on page 301.

### Example

This example shows how to set the maximum file size buffered to memory for scanning at 25 MB, the maximum uncompressed file size that can be buffered to memory at 100 MB, and how to enable antivirus scanning on ports 20 and 21 for FTP traffic.

```
config antivirus service ftp
  set memfilesizelimit 25
  set uncompsizelimit 100
  set port 20 21
end
```

This example shows how to display the antivirus FTP traffic settings.

```
get antivirus service ftp
```

This example shows how to display the configuration for antivirus FTP traffic.

```
show antivirus service ftp
```

## config antivirus service pop3

Use this command to configure how the FortiGate unit handles antivirus scanning of large files in POP3 traffic and what ports the FortiGate unit scans for POP3.

### Command syntax pattern

```
config antivirus service pop3
  set <keyword> <variable>
end

config antivirus service pop3
  unset <keyword>
end

get antivirus service [pop3]

show antivirus service [pop3]
```

### antivirus service pop3 command keywords and variables

Keywords and variables	Description	Default	Availability
memfilesizelimit <MB_integer>	Set the maximum file size that can be buffered to memory for virus scanning. The maximum file size allowed is 10% of the FortiGate RAM size. For example, a FortiGate unit with 256 MB of RAM could have a threshold range of 1 MB to 25 MB. Note: For email scanning, the memfilesizelimit refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes less than the memfilesizelimit.	10 (MB)	All models.
port <port_integer>	Configure antivirus scanning on a nonstandard port number or multiple port numbers for POP3. You can use ports from the range 1-65535. You can add up to 20 ports.	110	All models.
uncompsizelimit <MB_integer>	Set the maximum uncompressed file size that can be buffered to memory for virus scanning. Enter a value in megabytes between 1 and the total memory size. Enter 0 for no limit (not recommended).	10 (MB)	All models.

### How file size limits work

See [“How file size limits work”](#) on page 301.



## Example

This example shows how to set the maximum file size that can be buffered to memory for scanning at 20 MB, the maximum uncompressed file size that can be buffered to memory for scanning at 60 MB, and how to enable antivirus scanning on ports 110, 111, and 992 for POP3 traffic.

```
config antivirus service pop3
    set memfilesizelimit 20
    set uncompsizelimit 60
    set port 110
    set port 111
    set port 992
end
```

This example shows how to display the antivirus POP3 traffic settings.

```
get antivirus service pop3
```

This example shows how to display the configuration for antivirus POP3 traffic.

```
show antivirus service pop3
```

## config antivirus service imap

Use this command to configure how the FortiGate unit handles antivirus scanning of large files in IMAP traffic and what ports the FortiGate unit scans for IMAP.

### Command syntax pattern

```
config antivirus service imap
    set <keyword> <variable>
end

config antivirus service imap
    unset <keyword>
end

get antivirus service [imap]
show antivirus service [imap]
```

## antivirus service imap command keywords and variables

Keywords and variables	Description	Default	Availability
memfilesizelimit <MB_integer>	Set the maximum file size that can be buffered to memory for virus scanning. The maximum file size allowed is 10% of the FortiGate RAM size. For example, a FortiGate unit with 256 MB of RAM could have a threshold range of 1 MB to 25 MB. Note: For email scanning, the memfilesizelimit refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes less than the memfilesizelimit.	10 (MB)	All models.
port <port_integer>	Configure antivirus scanning on a nonstandard port number or multiple port numbers for IMAP. You can use ports from the range 1-65535. You can add up to 20 ports.	143	All models.
uncompsizelimit <MB_integer>	Set the maximum uncompressed file size that can be buffered to memory for virus scanning. Enter a value in megabytes between 1 and the total memory size. Enter 0 for no limit (not recommended).	10 (MB)	All models.

### How file size limits work

See [“How file size limits work”](#) on page 301.

### Example

This example shows how to set the maximum file size that can be buffered to memory for scanning at 25 MB, the maximum uncompressed file size that can be buffered to memory for scanning at 50 MB, and how to enable antivirus scanning on ports 143 and 993 for IMAP traffic.

```
config antivirus service http
  set memfilesizelimit 25
  set uncompsizelimit 50
  set port 143
  set port 993
end
```

This example shows how to display the antivirus IMAP traffic settings.

```
get antivirus service imap
```

This example shows how to display the configuration for antivirus IMAP traffic.

```
show antivirus service imap
```

## config antivirus service smtp

Use this command to configure how the FortiGate unit handles antivirus scanning of large files in SMTP traffic, what ports the FortiGate unit scans for SMTP, and how the FortiGate unit handles interaction with an SMTP server for delivery of email with infected email file attachments.

### Command syntax pattern

```
config antivirus service smtp
  set <keyword> <variable>
end

config antivirus service smtp
  unset <keyword>
end

get antivirus service [smtp]

show antivirus service [smtp]
```

### antivirus service smtp command keywords and variables

Keywords and variables	Description	Default	Availability
memfilesizelimit <MB_integer>	Set the maximum file size that can be buffered to memory for virus scanning. The maximum file size allowed is 10% of the FortiGate RAM size. For example, a FortiGate unit with 256 MB of RAM could have a threshold range of 1 MB to 25 MB. Note: For email scanning, the memfilesizelimit refers to the final size of the email after encoding by the email client, including attachments. Email clients may use a variety of encoding types and some encoding types translate into larger file sizes than the original attachment. The most common encoding, base64, translates 3 bytes of binary data into 4 bytes of base64 data. So a file may be blocked or logged as oversized even if the attachment is several megabytes less than the memfilesizelimit.	10 (MB)	All models.
port <port_integer>	Configure antivirus scanning on a nonstandard port number or multiple port numbers for SMTP. You can use ports from the range 1-65535. You can add up to 20 ports.	143	All models.
uncompsizelimit <MB_integer>	Set the maximum uncompressed file size that can be buffered to memory for virus scanning. Enter a value in megabytes between 1 and the total memory size. Enter 0 for no limit (not recommended).	10 (MB)	All models.

### How file size limits work

See [“How file size limits work”](#) on page 301.

## Example

This example shows how to set the maximum file size that can be buffered to memory for scanning at 100 MB, the maximum uncompressed file size that can be buffered to memory for scanning at 1 GB (1000 MB), and how to enable antivirus scanning on ports 25, and 465 for SMTP traffic.

```
config antivirus service smtp
  set memfilesizelimit 100
  set uncompsizelimit 1000
  set port 25
  set port 465
end
```

This example shows how to display the antivirus SMTP traffic settings.

```
get antivirus service smtp
```

This example shows how to display the configuration for antivirus SMTP traffic.

```
show antivirus service smtp
```

# Web filter

Web filter provides configuration access to the Web filtering and Web category filtering options you enable when you create a firewall Protection Profile.

To access protection profile web filter options go to Firewall > Protection Profile, select edit or Create New, and select Web Filtering or Web Category Filtering. See [“Protection profile options” on page 223](#).

**Table 27: Web filter and Protection Profile web filtering configuration**

Protection Profile web filtering options	Web Filter setting
Web Content Block	Web Filter > Content Block
Enable or disable web page blocking based on the banned words and patterns in the content block list for HTTP traffic.	Add words and patterns to block web pages containing those words or patterns.
Web URL Block	Web Filter > URL Block
Enable or disable web page filtering for HTTP traffic based on the URL block list.	Add URLs and URL patterns to block web pages from specific sources.
Web Exempt List	Web Filter > URL Exempt
Enable or disable web page filtering for HTTP traffic based on the URL exempt list. Exempt URLs are not scanned for viruses.	Add URLs to exempt them from web and virus filtering.
Web Script Filter	Web Filter > Script Filter
Enable or disable blocking scripts from web pages for HTTP traffic.	Select the scripts to block.
Web resume download block	
Enable to block downloading parts of a file that have already been partially downloaded. Enabling this option will prevent the unintentional download of virus files, but can cause download interruptions.	

**Table 28: Web filter and Protection Profile web category filtering configuration**

Protection Profile web category filtering	Web Filter setting
Enable category block (HTTP only)	Web Filter > Category Block > Configuration
Enable FortiGuard web filtering.	Enable or disable FortiGuard and enable and set the size limit for the cache.
Block unrated websites (HTTP only)	
Block any web pages that have not been rated by the FortiGuard.	
Allow websites when a rating error occurs (HTTP only)	
Allow web pages that return a rating error from FortiGuard.	
Category / Action	
FortiGuard web filtering service provides many categories by which to filter web traffic. You can set the action to take on web pages for each category. Choose from allow, monitor, or reject.	

## Protection profile configuration

For information about configuring Protection Profiles, see [“Protection profile” on page 222](#). For information about adding protection profiles to firewall policies, see [“To add a protection profile to a policy” on page 229](#).

## Order of web filter operations

Web filtering includes various modules and engines that perform separate tasks. The FortiGate unit performs web filtering in the order the filters appear in the web-based manager menu: content block, URL block, URL exempt, category block (FortiGuard), and script filter.

This chapter describes:

- [Content block](#)
- [URL block](#)
- [URL exempt](#)
- [Category block](#)
- [Script filter](#)

## Content block

Control web content by blocking specific words or word patterns. The FortiGate unit blocks web pages containing banned words and displays a replacement message instead.

You can use Perl regular expressions or wildcards to add banned word patterns to the list. See [“Using Perl regular expressions” on page 335](#).



**Note:** Perl regular expression patterns are case sensitive for Web Filter content block. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

This section describes:

- [Web content block list](#)
- [Web content block options](#)
- [Configuring the web content block list](#)

### Web content block list

You can add one or more banned words or patterns to block web pages containing those words. Banned words can be one word or a text string up to 80 characters long. The maximum number of banned words in the list is 32.

**Figure 160:Sample Web Content Block List, banned words**

Create New		total: 4			
<input checked="" type="checkbox"/> Banned Word	Pattern Type	Language			
<input checked="" type="checkbox"/> very bad word	Wildcard	Western			
<input checked="" type="checkbox"/> mauvais mot	Wildcard	French			
<input checked="" type="checkbox"/> ^porn	Regular Expression	Western			
<input checked="" type="checkbox"/> porn*	Wildcard	Western			



**Note:** Enable Web filtering > Web Content Block in your firewall Protection Profile to activate the content block settings.

### Web content block options

Web content block has the following icons and features:

<b>Create new</b>	Select Create New to add a banned word to the web content block list.
<b>total</b>	The number of banned words in the web content block list. Page up, Page down, and Clear banned word list icons.
<b>Banned word</b>	The current list of banned words and patterns. Select the check box to enable all the banned words in the list.
<b>Pattern type</b>	The pattern type used in the banned word list entry. Choose from wildcard or regular expression. See <a href="#">“Using Perl regular expressions” on page 335</a> .
<b>Language</b>	The character set to which the banned word belongs: Simplified Chinese, Traditional Chinese, French, Japanese, Korean, Thai, or Western. The Delete and Edit/View icons.

## Configuring the web content block list

Figure 161: Adding a banned word to the content block list

When you select Create New or Edit you can configure the following settings for the banned word.

- Banned word** Enter the word or pattern you want to include in the banned word list
- Pattern type** Select the pattern type for the banned word. Choose from wildcard or regular expression. See ["Using Perl regular expressions" on page 335](#).
- Language** Select the character set for the banned word. Choose from: Chinese Simplified, Chinese Traditional, French, Japanese, Korean, Thai, or Western.
- Enable** Select Enable to activate the banned word in the list.

### To add or edit a banned word

- 1 Go to **Web Filter > Content Block**.
- 2 Select Create New to add a banned word or select Edit for the banned word you want to modify.
- 3 Enter the word or phrase.  
If you enter a single word, the FortiGate unit blocks all web pages that contain that word. If you enter a phrase, the FortiGate unit blocks all web pages containing any word in the phrase. If you contain the phrase in quotation marks, the FortiGate unit blocks all web pages containing the exact phrase.
- 4 Set the pattern type if required.
- 5 Select the language (character set).
- 6 Select Enable.
- 7 Select OK.

## URL block

You can block access to specific URLs by adding them to the URL block list. You can also add patterns using text and regular expressions (or wildcard characters) to block URLs. The FortiGate unit blocks web pages matching any specified URLs or patterns and displays a replacement message instead.



**Note:** Enable Web filtering > Web URL Block in your firewall Protection Profile to activate the URL block settings.





**Note:** URL blocking does not block access to other services that users can access with a web browser. For example, URL blocking does not block access to `ftp://ftp.badsite.com`. Instead, you can use firewall policies to deny FTP connections.

This section describes:

- [Web URL block list](#)
- [Web URL block options](#)
- [Configuring the web URL block list](#)
- [Web pattern block list](#)
- [Web pattern block options](#)
- [Configuring web pattern block](#)

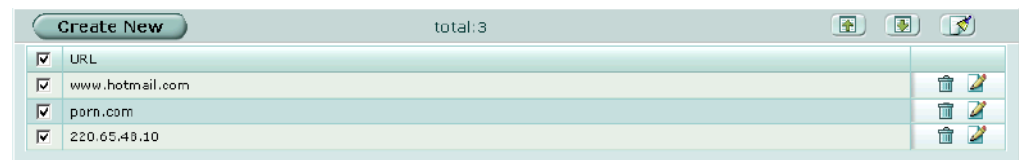
## Web URL block list

You can add your own specific URLs to block or you can obtain one of several publicly available lists of objectionable URLs. You can add the following items to the URL block list:

- complete URLs
- IP addresses
- partial URLs to block all sub-domains

If you want to use more than one URL block list, simply combine the lists in a text file and upload them to the FortiGate unit by selecting the Upload URL block list icon. URLs in a text file must be separated by hard returns to upload correctly.

**Figure 162: Sample Web URL block list**



## Web URL block options

Web URL block has the following icons and features:

<b>Create New</b>	Select Create New to add a URL to the URL block list.
<b>total</b>	The number of URLs in the URL block list. The Page up, Page down, and Clear URL block list icons.
<b>URL</b>	The current list of blocked URLs. Select the check box to enable all the URLs in the list. The Delete and Edit/View icons.

## Configuring the web URL block list



**Note:** Do not use regular expressions in the web URL block list. You can use regular expressions in the web pattern block list to create URL patterns to block. See [“Web pattern block list” on page 314](#).



**Note:** You can type a top-level domain suffix (for example, “com” without the leading period) to block access to all URLs with this suffix.

### To add a URL to the web URL block list

- 1 Go to **Web Filter > URL Block**.
- 2 Select Web URL Block.
- 3 Select Create New.

**Figure 163:** Adding a new URL

- 4 Enter a URL or partial URL to add to the URL block list. (Do not include http://.)  
Type a top-level URL or IP address to block access to all pages on a web site. For example, `www.badsite.com` or `122.133.144.155` blocks access to all pages at this web site.  
Enter a top-level URL followed by the path and filename to block access to a single page on a web site. For example, `www.badsite.com/news.html` or `122.133.144.155/news.html` blocks the news page on this web site.  
To block all pages with a URL that ends with `badsite.com`, add `badsite.com` to the block list. For example, adding `badsite.com` blocks access to `www.badsite.com`, `mail.badsite.com`, `www.finance.badsite.com`, and so on.
- 5 Select Enable.
- 6 Select OK.

## Web pattern block list

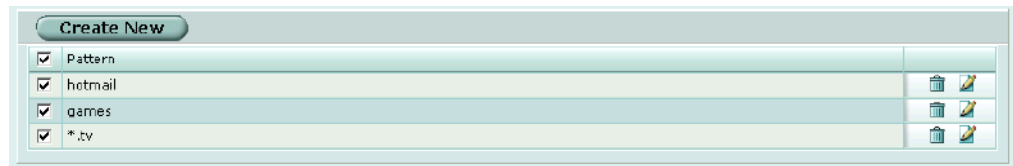
In addition to blocking specific or partial URLs, you can block all URLs that match patterns you create using text and regular expressions (or wildcard characters). For example, `badsite.*` matches `badsite.com`, `badsite.org`, `badsite.net` and so on.

FortiGate web pattern blocking supports standard regular expressions. You can add up to 20 patterns to the web pattern block list.



**Note:** Enable Web filtering > Web URL Block in your firewall Protection Profile to activate the web pattern block settings.

Figure 164: Sample web pattern block list



## Web pattern block options

Web pattern block has the following icons and features:

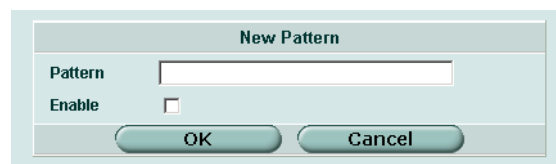
- Create New** Select Create New to add a new pattern to the web pattern block list.
- Pattern** The current list of blocked patterns. Select the check box to enable all the web patterns in the list.
- The Delete and Edit/View icons.

## Configuring web pattern block

### To add a pattern to the web pattern block list

- 1 Go to **Web Filter > URL Block**.
- 2 Select Web Pattern Block.
- 3 Select Create New.

Figure 165: Adding a new pattern



- 4 Enter a pattern to add to the web pattern block list.
- 5 Select Enable.
- 6 Select OK.

## URL exempt



**Note:** URLs in the URL exempt list bypass all security features, including virus scanning.

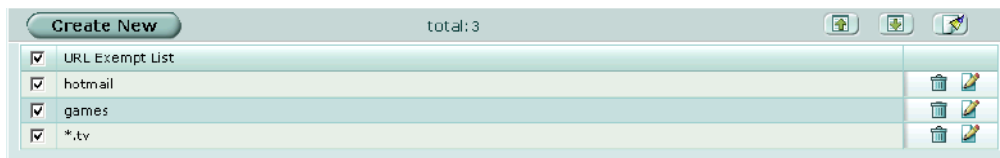
This section describes:

- [URL exempt list](#)
- [URL exempt list options](#)
- [Configuring URL exempt](#)

## URL exempt list

You can configure specific URLs as exempt from web filtering. URLs on the exempt list are not scanned for viruses. If users on your network download files through the FortiGate unit from trusted website, you can add the URL of this website to the exempt list so that the FortiGate unit does not virus scan files downloaded from this URL.

**Figure 166:Sample URL exempt list**



**Note:** Enable Web filtering > Web Exempt List in your firewall Protection Profile to activate the URL exempt settings.

## URL exempt list options

URL exempt list has the following icons and features:

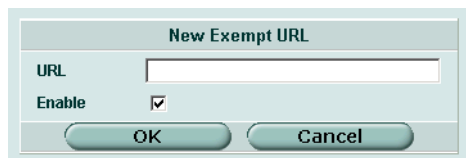
- Create New** Select Create New to add a URL to the URL exempt list.
- total** The number of URLs in the URL exempt list.
- Page up icon** Select this icon to scroll the URL exempt list up.
- Page down icon** Select this icon to scroll the URL exempt list down.
- Clear URL exempt list icon** Select this icon to delete the entire URL exempt list.
- URL Exempt List** The current list of exempt URLs. Select the check box to enable all the URLs in the list.  
The Delete and Edit/View icons.

## Configuring URL exempt

### To add a URL to the URL exempt list

- 1 Go to **Web Filter > URL Exempt**.
- 2 Select Create New.

**Figure 167:Adding a new exempt URL**



- 3 Enter the URL to add to the URL exempt list.
- 4 Select Enable.
- 5 Select OK.

## Category block

You can filter http content by specific categories using the FortiGuard managed web filtering service.

This section describes:

- [FortiGuard managed web filtering service](#)
- [Category block configuration options](#)
- [Category block reports](#)
- [Category block reports options](#)
- [Generating a category block report](#)
- [Category block CLI configuration](#)

### FortiGuard managed web filtering service

FortiGuard is a managed web filtering solution provided by Fortinet. FortiGuard sorts hundreds of millions of web pages into a wide range of categories that users can allow, block, or monitor. The FortiGate unit accesses the nearest FortiGuard Service Point to determine the category of a requested web page and then follows the firewall policy configured for that user or interface.

### FortiGuard categories and ratings

FortiGuard includes over 60 million individual ratings of web sites applying to hundreds of millions of pages. Pages are rated into 56 categories that users can allow, block, or monitor. Categories may be added to or updated as the Internet evolves. Users can also choose to allow, block, or monitor entire groups of categories to make configuration simpler. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

FortiGuard ratings are performed by a combination of proprietary methods including text analysis, exploitation of the Web structure, and human raters. Users can notify the FortiGuard Service Points if they feel a web page is not categorized correctly, and new sites are quickly rated as required.

See [“FortiGuard categories” on page 359](#) for a complete list and description of the FortiGuard web filter categories.

### FortiGuard Service Points

FortiGuard Service Points provide worldwide coverage. By default, the FortiGate unit will communicate with the closest Service Point. If the Service Point becomes unreachable for any reason, the FortiGate unit will contact another Service Point and rating information will be available within seconds. FortiGuard Service Points are highly scalable and new Service Points are added as required. The FortiGate unit communicates with the Service Point over UDP on port 8888. You can change the FortiGuard hostname if required, using the CLI. See [“Category block CLI configuration” on page 320](#).

## FortiGuard licensing

Every FortiGate unit comes with a free 30-day FortiGuard trial license. FortiGuard license management is done by Fortinet servers, so there is no need to enter a license number. The FortiGate unit will then automatically contact a FortiGuard Service Point when you enable FortiGuard category blocking.

When you want to renew your FortiGuard license after the free trial, contact Fortinet Technical Support.

## FortiGuard configuration

Once selected, FortiGuard category blocking is enabled globally. After enabling FortiGuard you can configure different categories for each firewall protection profile you create.

Use the procedure “[Configuring web category filtering options](#)” on page 225 to configure FortiGuard category blocking in a protection profile.

## Category block configuration options

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

**Figure 168:Category block configuration**

You can configure the following options to enable and help maintain FortiGuard web filtering:

- Enable Service FortiGuard** Select to enable FortiGuard web filtering.  
Status: Select Check Status to test the connection to the FortiGuard server. Status should change from a flashing red/yellow indicator to a solid green indicator when the server is contacted successfully.  
License Type: The FortiGuard license type.  
Expiration: The date the FortiGuard license expires.
- Enable Cache** Select to enable caching of category ratings for accessed URLs. This means that the FortiGate unit does not have to contact the server each time a commonly requested URL is accessed. The cache is configured to use 6% of the of the FortiGate RAM. When the cache is full, the least recently accessed URL is deleted.

- TTL** Time to live. The number of seconds to store URL ratings in the cache before contacting the server again.
- To have a URL's...** To have a URL's category rating re-evaluated, please click here. Select the link to have a web site re-evaluated if you think the category rating is incorrect. You must provide a complete valid URL.

### Configuring web category block

#### To enable FortiGuard web filtering

- 1 Go to Web Filter > Category Block.
- 2 Select Enable Service.
- 3 Select Check status to make sure the FortiGate unit can access the FortiGuard server.  
After a moment, the FortiGuard status should change from Unknown to Available. If the FortiGuard status is unavailable, wait and try again.
- 4 Enable and set a TTL (time to live) for the cache.
- 5 Select Apply.

You can now enable web category blocking and configure categories for any firewall protection profile you create. See ["Configuring web category filtering options"](#) on page 225 and ["FortiGuard categories"](#) on page 359.

Once you select Apply, the FortiGuard license type and expiration date appears on the configuration screen (Web Filter > Category Block).

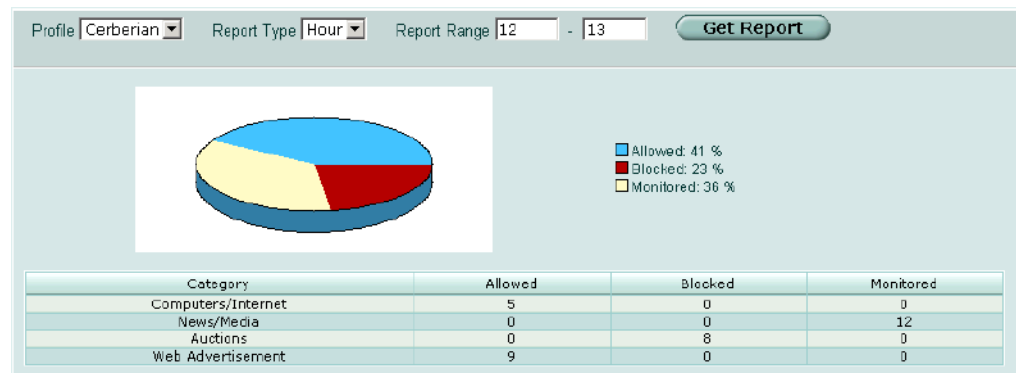
### Category block reports



**Note:** Category block reports are only available on FortiGate units with a local disk.

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

**Figure 169: Sample report**



## Category block reports options

The following table describes the options for generating reports:

<b>Profile</b>	Select the profile for which you want to generate a report.
<b>Report Type</b>	Select the time frame for which you want to generate the report. Choose from hour, day, or all historical statistics.
<b>Report Range</b>	Select the time range (24 hour clock) or day range (from six days ago to today) for which you want the report. For example, if you select report type hour and enter the range 13 – 16 you will get a category block report for 1 pm to 4 pm today. If you select report type day and enter range 0 – 3 you will get a category block report for 3 days ago to today.
<b>Get Report</b>	Select Get Report to generate the report.

The following table describes the features of a generated report:

<b>Category</b>	The category for which the statistic was generated.
<b>Allowed</b>	The number of allowed web addresses accessed in the selected time frame.
<b>Blocked</b>	The number of blocked web addresses accessed in the selected time frame.
<b>Monitored</b>	The number of monitored web addresses accessed in the selected time frame.

## Generating a category block report

### To generate a category block report

- 1 Go to **Web filter > Category block**.
- 2 Select Reports.
- 3 Select a profile for which to generate the report.
- 4 Select a report type.
- 5 Enter a report range.
- 6 Select Get Report.

The report is generated, including a pie chart and a list of web pages blocked by category.

## Category block CLI configuration

Use the `ftgd_hostname` keyword for the `webfilter catblock` command if you ever need to change the default hostname (URL) for the FortiGuard Service Point. The FortiGuard Service Point name cannot be changed using the web-based manager. You can configure all the FortiGuard settings using from the CLI. See the *FortiGate CLI Reference Guide* for descriptions of all `webfilter catblock` keywords.



**Note:** This command has more keywords than are listed in this Guide. See the *FortiGate CLI Reference Guide* for a complete list of commands and keywords.



## Command syntax pattern

```

config webfilter catblock
    set <keyword> <variable>
end

config webfilter catblock
    unset <keyword>
end

get webfilter catblock

show webfilter catblock

```

## catblock command keywords and variables

Keywords and variables	Description	Default	Availability
ftgd_hostname <url_str>	The hostname of the FortiGuard Service Point. The FortiGate comes preconfigured with the host name. Use this command only if you need to change the host name.	guard.fortinet.com	All models. service fortiguar d only.

## Example

This example shows how to change the FortiGuard Service Point name.

```

config webfilter catblock
    set ftgd_hostname guard.example.net
end

```

This example shows how to display the catblock settings.

```
get webfilter catblock
```

This example shows how to display the configuration for the catblock settings.

```
show webfilter catblock
```

If the show command returns you to the prompt, the settings are at default.

## Script filter

You can configure the FortiGate unit to filter certain web scripts. You can filter Java applets, cookies, and ActiveX controls from web pages.

Figure 170:Script filtering options



**Note:** Blocking any of these items may prevent some web pages from functioning and displaying correctly.



**Note:** Enable Web filtering > Web Script Filter in your firewall Protection Profile to activate the script filter settings.

## Web script filter options

You can configure the following options for script filtering:

- |                   |   |
|-------------------|---|
| <b>Javascript</b> | Select Javascript to block all Javascript-based pages or applications.          |
| <b>Cookies</b>    | Select Cookies to block web sites from placing cookies on individual computers. |
| <b>ActiveX</b>    | Select ActiveX to block all ActiveX applications.                               |

# Spam filter

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

[Table 29](#) describes the spam filter settings and where to configure and access them. To access protection profile spam filter options go to Firewall > Protection Profile, edit or Create New, Spam Filtering. See [“Protection profile options” on page 223](#).

**Table 29: Spam Filter and Protection Profile spam filtering configuration**

Protection Profile spam filtering options	Spam filter setting
IP address FortiShield check	Spam Filter > FortiShield
Enable or disable Fortinet’s antispam service: FortiShield. This service works like an RBL server and is continuously updated to block spam sources.	Check the status of the FortiShield server, view the license type and expiry date, and configure the cache.
IP address BWL check	Spam Filter > IP Address
Black/white list check. Enable or disable checking incoming IP addresses against the configured spam filter IP address list. (SMTP only.)	Add to and edit IP addresses to the list. You can configure the action to take as spam, clear, or reject for each IP address. You can place an IP address anywhere in the list. The filter checks each IP address in sequence. (SMTP only.)
RBL & ORDBL check	Spam Filter > RBL & ORDBL
Enable or disable checking SMTP traffic against configured Real-time Blackhole List and Open Relay Database List servers.	Add to and edit RBL and ORDBL servers to the list. You can configure the action to take as spam or reject for email identified as spam from each server. (SMTP only.)
HELO DNS lookup	
Enable or disable checking the source domain name against the registered IP address in the Domain Name Server. If the source domain name does not match the IP address the email is marked as spam and the action selected in the protection profile is taken.	

**Table 29: Spam Filter and Protection Profile spam filtering configuration**

Protection Profile spam filtering options	Spam filter setting
<b>E-mail address BWL check</b>	Spam Filter > E-mail Address
Enable or disable checking incoming email addresses against the configured spam filter email address list.	Add to and edit email addresses to the list, with the option of using wildcards and regular expressions. You can configure the action to take as spam or reject for each email address. You can place an email address anywhere in the list. The filter checks each email address in sequence.
<b>Return e-mail DNS check</b>	
Enable or disable checking incoming email return address domain against the registered IP address in the Domain Name Server. If the return address domain name does not match the IP address the email is marked as spam and the action selected in the protection profile is taken.	
<b>MIME headers check</b>	Spam Filter > MIME Headers
Enable or disable checking source MIME headers against the configured spam filter MIME header list.	Add to and edit MIME headers to the list, with the option of using wildcards and regular expressions. You can configure the action to take as spam or clear for each MIME header.
<b>Banned word check</b>	Spam Filter > Banned Word
Enable or disable checking source email against the configured spam filter banned word list.	Add to and edit banned words to the list, with the option of using wildcards and regular expressions. You can configure the language and whether to search the email body, subject, or both. You can configure the action to take as spam or clear for each word.
<b>Spam Action</b>	
The action to take on email identified as spam. POP3 and IMAP messages are tagged. Choose Tagged or Discard for SMTP messages. You can append a custom word or phrase to the subject or MIME header of tagged email. You can choose to log any spam action in the event log.	
<b>Append to:</b>	
Choose to append the tag to the subject or MIME header of the email identified as spam.	
<b>Append with:</b>	
Enter a word or phrase (tag) to append to email identified as spam. The maximum length is 63 characters.	
<b>Add event into the system log</b>	
Enable or disable logging of spam actions to the event log.	

## Protection profile configuration

For information about configuring protection profiles, see [“Protection profile” on page 222](#). For information about adding protection profiles to firewall policies, see [“To add a protection profile to a policy” on page 229](#).

## Order of spam filter operations

Generally, incoming email is passed through the spam filters in the order the filters appear in the spam filtering options list in a firewall protection profile (and in [Table 29](#)): FortiShield, IP address, RBL & ORDBL, HELO DNS lookup, email address, return email DNS check, MIME header, and banned word (content block). Each filter passes the email to the next if no matches or problems are found. If the action in the filter is Mark as Spam, the FortiGate unit will tag or discard (SMTP only) the email according to the settings in the protection profile. If the action in the filter is Mark as Clear, the email is exempt from any remaining filters. If the action in the filter is Mark as Reject, the email session is dropped. Rejected SMTP email messages are substituted with a configurable replacement message. See [“Replacement messages” on page 105](#).

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

This chapter describes:

- [FortiShield](#)
- [IP address](#)
- [RBL & ORDBL](#)
- [Email address](#)
- [MIME headers](#)
- [Banned word](#)
- [Using Perl regular expressions](#)

## FortiShield

FortiShield is an antispam system from Fortinet that uses an IP address black list and spam filtering tools. FortiShield compiles the IP address list from email captured by spam probes located around the world. Spam probes are email addresses purposely configured to attract spam and identify known spam sources to create the antispam IP address list. FortiShield combines IP address checks with other spam filter techniques in a two-pass process.

On the first pass, FortiShield checks the SMTP mail server source address against the antispam IP address list. If the source address matches the list of known spammers, FortiShield terminates the session. If FortiShield does not find a match, the mail server sends the email to the recipient.

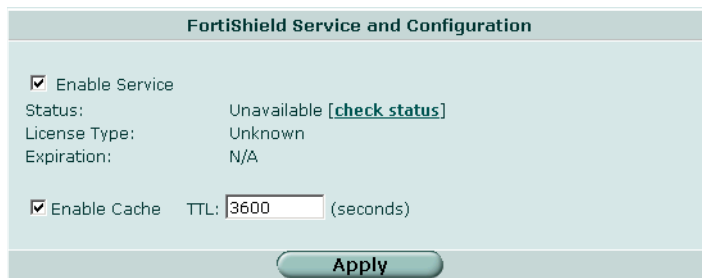
As each email is received, FortiShield performs the second antispam pass by checking the header, subject, and body of the email for common spam content. If FortiShield finds spam content, the email is tagged or dropped according to the configuration in the firewall protection profile.

Both FortiShield antispam processes are completely automated and configured by Fortinet. With constant monitoring and dynamic updates, FortiShield is always current. You can enable or disable FortiShield in a firewall protection profile. See [“Configuring spam filtering options” on page 226](#).

### FortiShield options

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

**Figure 171:FortiShield configuration**



You can configure or view the following settings for the FortiShield service:

- Enable Service** Select to enable the FortiShield service.
- Status** Select Check Status to test the connection to the FortiShield server. Status should change from a flashing red/yellow indicator to a solid green indicator when the server is contacted successfully.
- License Type** The FortiShield license type.
- Expiration** The date the FortiShield license expires.
- Enable Cache** Select to enable caching of listings from the IP address block list in FortiShield. This means that the FortiGate unit does not have to contact the server each time the same IP address appears as the source of an email. The cache is configured to use 6% of the of the FortiGate RAM. When the cache is full, the least recently used IP address is deleted.
- TTL** Time to live. The number of seconds to store blocked IP addresses in the cache before contacting the server again.

### Configuring the FortiShield cache

- 1 Go to Spam Filter > FortiShield.
- 2 Select Check status to make sure the FortiGate unit can access the FortiShield server.  
After a moment, the FortiShield status should change from Unknown to Available. If the FortiShield status is unavailable, wait and try again.
- 3 Enable and set a TTL (time to live) for the cache.

#### 4 Select Apply.

You can now enable FortiShield for any firewall protection profile you create. See [“Configuring spam filtering options” on page 226](#).

Once you select Apply, the FortiShield license type and expiration date appears on the configuration screen (Spam Filter > FortiShield).

## IP address

The FortiGate unit uses the IP address list to filter incoming email. The FortiGate unit compares the IP address of the sender to the list in sequence. If a match is found, the corresponding protection profile action is taken. If no match is found, the email is passed on to the next spam filter.

You can enter an IP address and mask in two formats:

- x.x.x.x/x.x.x.x, for example 62.128.69.100/255.255.255.0
- x.x.x.x/x, for example 62.128.69.100/24

This section describes:

- [IP address list](#)
- [IP address options](#)
- [Configuring the IP address list](#)

### IP address list

You can configure the FortiGate unit to filter email from specific IP addresses. You can mark each IP address as clear, spam, or reject. You can filter single IP addresses, or a range of addresses at the network level by configuring an address and mask.

**Figure 172: Sample IP address list**

Create New		Total: 4		
<input checked="" type="checkbox"/>	IP Address / Mask	Action		
<input checked="" type="checkbox"/>	172.18.72.0/24	Spam		
<input checked="" type="checkbox"/>	192.168.65.99	Clear		
<input checked="" type="checkbox"/>	10.0.0.0/8	Reject		
<input checked="" type="checkbox"/>	172.30.0.0/16	Spam		

### IP address options

IP address list has the following icons and features:

<b>Create New</b>	Select Create New to add an IP address to the IP address list.
<b>Total</b>	The number of items in the list.
	The Page up, Page down, and Remove all entries icons.
<b>IP address/Mask</b>	The current list of IP addresses.

<b>Action</b>	The action to take on email from the configured IP address. Actions are: Mark as Spam to apply the spam action configured in the protection profile, Mark as Clear to let the email pass to the next filter, or Mark as Reject (SMTP only) to drop the session.  The Delete and Edit/View icons.
---------------	--

## Configuring the IP address list

### To add an IP address to the IP address list

- 1 Go to **Spam Filter > IP Address**.
- 2 Select Create New.

**Figure 173: Adding an IP address**

- 3 Enter the IP address/mask you want to add.
- 4 If required, select before or after another IP address in the list to place the new IP address in the correct position.
- 5 Select the action to take on email from the IP address.
- 6 Select OK.

## RBL & ORDBL

Using RBLs (Real-time Blackhole Lists) and ORDBLs (Open Relay Database Lists) is an effective way to tag or reject spam as it enters your system. These lists act as domain name servers that match the domain of incoming email to a list of IP addresses known to send spam or allow spam to pass through. RBLs keep track of reported spam source addresses and ORDBLs keep track of unsecured third party SMTP servers, known as open relays, which some spammers use to send unsolicited bulk email.

There are also several free and subscription servers available that provide reliable access to continually updated RBLs and ORDBLs. Check with the service you are using to confirm the correct domain name for connecting to the server.

The FortiGate unit communicates with RBL servers using UDP through port 53. The FortiGate unit compares the IP address or domain name of the sender to any database lists you configure. The FortiGate unit checks all the servers in the list simultaneously. If a match is found, the corresponding protection profile action is taken. If no match is found, the email is passed on to the next spam filter.





**Note:** Because the FortiGate unit uses the server domain name to connect to the RBL or ORDBL server, it must be able to look up this name on the DNS server. For information on configuring DNS, see [“DNS” on page 61](#).

This section describes:

- [RBL & ORDBL list](#)
- [RBL & ORDBL options](#)
- [Configuring the RBL & ORDBL list](#)

## RBL & ORDBL list

You can configure the FortiGate unit to filter email by accessing RBL or ORDBL servers. You can mark a match by each server as spam or reject.

**Figure 174: Sample RBL & ORDBL list**

Create New		Total: 3		
<input checked="" type="checkbox"/>	RBL Server	Action		
<input checked="" type="checkbox"/>	list.dsbl.org	Spam		
<input checked="" type="checkbox"/>	bl.spamcop.net	Reject		
<input checked="" type="checkbox"/>	releys.ordb.org	Spam		

## RBL & ORDBL options

RBL & ORDBL list has the following icons and features:

<b>Create New</b>	Select Create New to add a server to the RBL & ORDBL list.
<b>Total</b>	The number of items in the list. The Page up, Page down, and Remove all entries icons.
<b>RBL Server</b>	The current list of servers. Select the check box to enable all the RBL and ORDBL servers in the list
<b>Action</b>	The action to take on email matched by the RBLs and ORDBLs. Actions are: Mark as Spam to apply the spam action configured in the protection profile, or Mark as Reject to drop the session. The Delete and Edit/View icons.

## Configuring the RBL & ORDBL list

**To add a server to the RBL & ORDBL list**

- 1 Go to **Spam Filter > RBL & ORDBL**.
- 2 Select Create New.

Figure 175: Adding an RBL or ORDBL server

- 3 Enter the domain name of the RBL or ORDBL server you want to add.
- 4 Select the action to take on email matched by the server.
- 5 Select Enable.
- 6 Select OK.

## Email address

The FortiGate unit uses the email address list to filter incoming email. The FortiGate unit compares the email address or domain of the sender to the list in sequence. If a match is found, the corresponding protection profile action is taken. If no match is found, the email is passed on to the next spam filter.

You can use Perl regular expressions or wildcards to add email address patterns to the list. See [“Using Perl regular expressions” on page 335](#).

This section describes:

- [Email address list](#)
- [Email address options](#)
- [Configuring the email address list](#)

### Email address list

The FortiGate unit can filter email from specific senders or all email from a domain (such as sample.net). You can mark each email address as clear or spam.

Figure 176: Sample email address list

Create New		Total: 3			
✓	E-mail Address	Pattern Type	Action		
✓	loser@spammer/.com	Regular Expression	Spam	🗑️	📄
✓	example.*	Wildcard	Spam	🗑️	📄
✓	*@fortinet.com	Wildcard	Clear	🗑️	📄

### Email address options

Email address list has the following icons and features:

- |                   |  |
|-------------------|--|
| <b>Create New</b> | Select Create New to add an email address to the email address list. |
| <b>Total</b>      | The number of items in the list.                                     |
|                   | The Page up, Page down, and Remove all entries icons.                |

<b>Email address</b>	The current list of email addresses.
<b>Pattern Type</b>	The pattern type used in the email address entry. Choose from wildcard or regular expression. See <a href="#">“Using Perl regular expressions” on page 335</a> .
<b>Action</b>	The action to take on email from the configured address. Actions are: Mark as Spam to apply the spam action configured in the protection profile, or Mark as Clear to let the email pass to the next filter. The Delete and Edit/View icons.

## Configuring the email address list

### To add an email address or domain to the list

- 1 Go to **Spam Filter > E-mail Address**.
- 2 Select Create New.

Figure 177: Adding an email address

- 3 Enter the email address or pattern you want to add.
- 4 Select a pattern type for the list entry.
- 5 If required, select before or after another email address in the list to place the new email address in the correct position.
- 6 Select the action to take on email from the configured address or domain.
- 7 Select OK.

## MIME headers

MIME (Multipurpose Internet Mail Extensions) headers are added to email to describe content type and content encoding, such as the type of text in the email body or the program that generated the email. Some examples of MIME headers include:

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

The first part of the MIME header is called the header key, or just header. The second part is called the value. Spammers will often insert comments into header values or leave them blank. These malformed headers can fool some spam and virus filters.

You can use the MIME headers list to mark email from certain bulk mail programs or with certain types of content that are common in spam messages. You can choose to mark the email as spam or clear for each header you configure.

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

You can use Perl regular expressions or wildcards to add MIME header patterns to the list. See [“Using Perl regular expressions” on page 335](#).



**Note:** MIME header entries are case sensitive.

This section describes:

- [MIME headers list](#)
- [MIME headers options](#)
- [Configuring the MIME headers list](#)

## MIME headers list

You can configure the FortiGate unit to filter email with specific MIME header key-value pairs. You can mark each MIME header as clear or spam.

**Figure 178:Sample MIME headers list**

Create New		Total: 5				
<input checked="" type="checkbox"/>	Header	Value	Pattern Type	Action		
<input checked="" type="checkbox"/>	X-UIDL	*	Wildcard	Spam		
<input checked="" type="checkbox"/>	X-Distribution	bulk	Wildcard	Spam		
<input checked="" type="checkbox"/>	Content-Type	image/jpg	Wildcard	Spam		
<input checked="" type="checkbox"/>	Content-Type	text/plain	Wildcard	Clear		
<input checked="" type="checkbox"/>	X-Mailer	outgluck	Wildcard	Spam		

## MIME headers options

MIME headers list has the following icons and features:

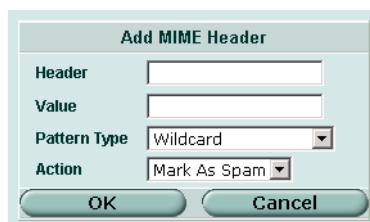
- Create New** Select Create New to add a MIME header to the MIME headers list.
- Total** The number of items in the list.  
The Page up, Page down, and Remove all entries icons.
- Header** The list of MIME headers (keys).
- Value** The list of MIME header values for each key.
- Pattern Type** The pattern type used in the MIME header list entry. Choose from wildcard or regular expression. See [“Using Perl regular expressions” on page 335](#).
- Action** The action to take on email with the configured MIME header. Actions are: Mark as Spam to apply the spam action configured in the protection profile, Mark as Clear to let the email pass to the next filter, or Mark as Reject (SMTP only) to drop the session.  
The Delete and Edit/View icons.

## Configuring the MIME headers list

### To add a MIME header to the list

- 1 Go to **Spam Filter > MIME headers**.
- 2 Select **Create New**.

Figure 179: Adding a MIME header



- 3 Enter the MIME header key.
- 4 Enter the MIME header value.
- 5 Select a pattern type for the list entry.
- 6 Select the action to take on email with that MIME header key-value.
- 7 Select **OK**.

## Banned word

Control spam by blocking email containing specific words or patterns. The FortiGate unit searches for banned words in email messages. If a match is found, the corresponding protection profile action is taken. If no match is found, the email is passed to the recipient.

You can use Perl regular expressions or wildcards to add banned word patterns to the list. See [“Using Perl regular expressions” on page 335](#).



**Note:** Perl regular expression patterns are case sensitive for Spam Filter banned words. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` will block all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

This section describes:

- [Banned word list](#)
- [Banned word options](#)
- [Configuring the banned word list](#)

## Banned word list

You can add one or more banned words to sort email containing those words in the email subject, body, or both.

Words can be marked as spam or clear. Banned words can be one word or a phrase up to 127 characters long.

If you enter a single word, the FortiGate unit blocks all email that contain that word. If you enter a phrase, the FortiGate unit blocks all email containing the exact phrase. To block any word in a phrase, use Perl regular expressions. See [“Using Perl regular expressions” on page 335](#).

**Figure 180:Sample banned word List**

<input checked="" type="checkbox"/>	Pattern	Pattern Type	Language	Where	Action	
<input checked="" type="checkbox"/>	'great deals'	Wildcard	Western	All	Spam	
<input checked="" type="checkbox"/>	'gratuit!'	Wildcard	French	Subject	Spam	
<input checked="" type="checkbox"/>	erotic\s+sex\s+story\ {(img jpg gif bmp wmv mov)}	Regular Expression	Western	All	Spam	
<input checked="" type="checkbox"/>	/^.*v.*i.*a.*g.*r.*a.*\$/i	Regular Expression	Western	All	Spam	

## Banned word options

Banned word has the following icons and features:

<b>Create new</b>	Select Create New to add a word or phrase to the banned word list.
<b>Total</b>	The number of items in the list. The Page up, Page down, and Remove all entries icons.
<b>Pattern</b>	The list of banned words. Select the check box to enable all the banned words in the list.
<b>Pattern Type</b>	The pattern type used in the banned word list entry. Choose from wildcard or regular expression. See <a href="#">“Using Perl regular expressions” on page 335</a> .
<b>Language</b>	The character set to which the banned word belongs: Simplified Chinese, Traditional Chinese, French, Japanese, Korean, Thai, or Western.
<b>Where</b>	The location which the FortiGate unit searches for the banned word: subject, body, or all.
<b>Action</b>	The selected action to take on email with banned words. The Delete and Edit/View icons.

When you select Create New or Edit you can configure the following settings for the banned word.

Figure 181: Adding a banned word

<b>Pattern</b>	Enter the word or phrase you want to include in the banned word list.
<b>Pattern Type</b>	Select the pattern type for the banned word. Choose from wildcard or regular expression. See <a href="#">“Using Perl regular expressions” on page 335</a> .
<b>Language</b>	Select the character set for the banned word. Choose from: Chinese Simplified, Chinese Traditional, French, Japanese, Korean, Thai, or Western.
<b>Where</b>	Select the location to search for the banned word. Choose from: subject, body, or all.
<b>Action</b>	Select the action to perform on email containing the banned word. Choose from: Mark as Spam to apply the spam action configured in the protection profile, or Mark as Clear to allow the email (since Banned Word is the last filter).
<b>Enable</b>	Select to enable scanning for the banned word.

## Configuring the banned word list

### To add or edit a banned word

- 1 Go to **Spam Filter > Banned Word**.
- 2 Select Create New to add a banned word or select Edit for the banned word you want to modify.
- 3 Enter the word or phrase.
- 4 Select the language (character set).
- 5 Select the location.
- 6 Select the action to take on email containing the banned word.
- 7 Select Enable.
- 8 Select OK.

## Using Perl regular expressions

Email address list, MIME headers list, and banned word list entries can include wildcards or Perl regular expressions.

See <http://www.perldoc.com/perl5.8.0/pod/perlre.html> for detailed information about using Perl regular expressions.

## Regular expression vs. wildcard match pattern

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

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

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

- To mach fortinet.com, the regular expression should be: fortinet\.com

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

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

To match any character 0 or more times, use '.\*' where '.' means any character and the '\*' means 0 or more times. For example, the wildcard match pattern forti\*.com should therefore be fort.\*\.com.

## Word boundary

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

## Case sensitivity

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

**Table 30: Perl regular expression formats**

Expression	Matches
abc	abc (that exact character sequence, but anywhere in the string)
^abc	abc at the beginning of the string
abc\$	abc at the end of the string
a b	either of a and b
^abc abc\$	the string abc at the beginning or at the end of the string
ab{2,4}c	an a followed by two, three or four b's followed by a c
ab{2,}c	an a followed by at least two b's followed by a c
ab*c	an a followed by any number (zero or more) of b's followed by a c
ab+c	an a followed by one or more b's followed by a c
ab?c	an a followed by an optional b followed by a c; that is, either abc or ac
a.c	an a followed by any single character (not newline) followed by a c
a\.c	a.c exactly
[abc]	any one of a, b and c



**Table 30: Perl regular expression formats**

[Aa]bc	either of Abc and abc
[abc]+	any (nonempty) string of a's, b's and c's (such as a, abba, acbabcacaa)
[^abc]+	any (nonempty) string which does not contain any of a, b and c (such as defg)
\d\d	any two decimal digits, such as 42; same as \d{2}
/i	makes the pattern case insensitive. For example, /bad language/i blocks any instance of bad language regardless of case.
\w+	a "word": a nonempty sequence of alphanumeric characters and low lines (underscores), such as foo and 12bar8 and foo_1
100\s*mk	the strings 100 and mk optionally separated by any amount of white space (spaces, tabs, newlines)
abc\b	abc when followed by a word boundary (e.g. in abc! but not in abcd)
perl\B	perl when not followed by a word boundary (e.g. in perlert but not in perl stuff)
\x	tells the regular expression parser to ignore white space that is neither backslashed nor within a character class. You can use this to break up your regular expression into (slightly) more readable parts.
/x	used to add regexps within other text. If the first character in a pattern is forward slash '/', the '/' is treated as the delimiter. The pattern must contain a second '/'. The pattern between '/' will be taken as a regexp, and anything after the second '/' will be parsed as a list of regexp options ('i', 'x', etc). An error occurs if the second '/' is missing. In regular expressions, the leading and trailing space is treated as part of the regular expression.

## Examples

### To block any word in a phrase

```
/block|any|word/
```

### To block purposely misspelled words

Spammers often insert other characters between the letters of a word to fool spam blocking software.

```
/^.*v.*i.*a.*g.*r.*a.*$/i
```

```
/cr[eéèêë] [\+\-\*=<>\.\,;! \?%&S@^\^°\$/€\{\}\} () \[\]\|\|\_01]dit/i
```

### To block common spam phrases

The following phrases are some examples of common phrases found in spam messages.

```
/try it for free/i
```

```
/student loans/i
```

```
/you're already approved/i
```

```
/special [\+\-\*=<>\.\,;! \?%&~#S@^\^°\$/€\{\}\} () \[\]\|\|\_1]offer/i
```



# Log & Report

FortiGate units provide extensive logging capabilities for traffic, system and network protection functions. You can set the severity level of the messages that are logged, and you can choose the types of events that are logged.

All types of log messages, except traffic and content, can be saved in internal memory. If a hard disk drive is installed, all types of log messages can be saved to the hard disk. You can optionally upload hard disk logs to an external server when the log rolls.

FortiGate units support external logging to a FortiLog unit, WebTrends and other Syslog servers. For each log location you can configure log setting options including addressing information, logging severity level and log format. Log filters define the types of log messages saved to each location.

You can configure the FortiGate unit to send alert email to up to three recipients when selected events occur. It is not necessary for an event to be logged to trigger an alert email.

The FortiGate unit will collect and send log messages in alert emails according to the level and time intervals you configure in the alert email options. All collected messages are assembled in one alert email which is sent as soon the time interval is reached for a message at or above the configured level.

For example, if you set the level as Alert and the time interval for Emergency and Alert to 3 minutes, then all Alert and Emergency log messages collected are sent in a single email every three minutes. Log filters define the types of log messages sent as alert emails.

In the following example alert email, the alert email level is set to Alert. The two Alert level messages collected since the last Alert interval are sent in a single email.

Figure 182: Example alert email

```
From: admin@example.com
Sent: Tuesday, April 27, 2004 5:30 PM
To: example@test.com
Subject: Message meets Alert condition

Message meets Alert condition
2004-04-27 13:28:52 device_id=APS3012803033139 log_id=0101023002
type=event subtype=ipsec pri=notice loc_ip=172.16.81.2 loc_port=500
rem_ip=172.16.81.1 rem_port=500 out_if=dmz vpn_tunnel=ToDmz action=negotiate
init=local mode= stage=-112 dir=inbound status=success msg="Initiator: tunnel
172.16.81.1, transform=ESP_3DES, HMAC_SHA1"

Message meets Alert condition
2004-04-27 13:28:54 device_id=APS3012803033139 log_id=0101023004
type=event subtype=ipsec pri=notice loc_ip=172.16.81.2 loc_port=500
rem_ip=172.16.81.1 rem_port=500 out_if=dmz vpn_tunnel=ToDmz action=negotiate
init=local mode=quick stage=2 dir=outbound status=success msg="Initiator: sent
172.16.81.1 quick mode message #2 (DONE)"
```

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

This chapter describes:

- [Log config](#)
- [Log access](#)
- [CLI configuration](#)

## Log config

Use Log Config to configure log storage, alert emails and log filters.

This section describes:

- [Log Setting options](#)
- [Alert E-mail options](#)
- [Log filter options](#)
- [Configuring log filters](#)
- [Enabling traffic logging](#)

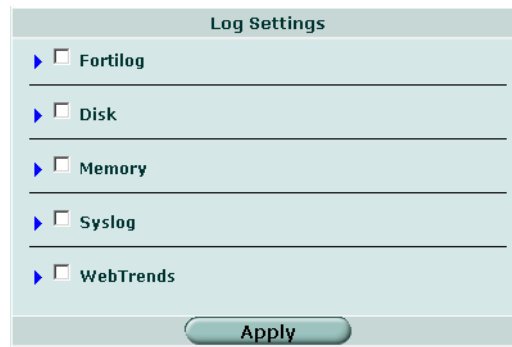
### Log Setting options

You can enable and configure the storing of log messages to one or more of the following locations:

**FortiLog** A FortiLog unit. The FortiLog unit is a log analyzer and manager that can combine the log information from various FortiGate units and other firewall units. To enable content archiving with a firewall [Protection profile](#), you need to select the FortiLog option and define its IP address.

<b>Disk</b>	The FortiGate disk (if the FortiGate unit has one).
<b>Memory</b>	The FortiGate system memory. The FortiGate system memory has a limited capacity and only displays the most recent log entries. Traffic and content logs cannot be stored in the memory buffer. When the memory is full, the FortiGate unit begins to overwrite the oldest messages. All log entries are deleted when the FortiGate unit restarts.
<b>Syslog</b>	A remote computer running a syslog server.
<b>WebTrends</b>	A remote computer running a NetIQ WebTrends firewall reporting server. FortiGate log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with NetIQ WebTrends Security Reporting Center 2.0 and Firewall Suite 4.1.

**Figure 183:Log setting options for all log locations**



### To configure Log Setting

- 1 Go to **Log&Report > Log Config > Log Setting**.
- 2 Select the check box to enable logging to a location.
- 3 Select the blue arrow beside the location.  
The setting options appear.
- 4 Enter the settings the logging location requires.
- 5 Repeat steps 2 through 8 to configure other logging locations.
- 6 Select Apply.

### FortiLog settings

IP:	The IP address of the FortiLog unit that manages the logs.
Level:	The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select Error, the unit logs Error, Critical, Alert and Emergency level messages. See <a href="#">Table 31, "Logging severity levels," on page 342</a> .
Enable encryption	Select to enable encryption of file transfer.
Local ID:	The identifier for the FortiGate unit. This must match the device name assigned to this unit on the FortiLog unit.
Pre-shared key	The pre-shared key used for encryption.

[Table 31](#) describes the FortiGate logging severity levels.

**Table 31: Logging severity levels**

Level	Description
Emergency	The system has become unstable.
Alert	Immediate action is required.
Critical	Functionality is affected.
Error	An error condition exists and functionality could be affected.
Warning	Functionality could be affected.
Notification	Notification of normal events.
Information	General information about system operations.

## Disk settings

Maximum size of log file	The maximum size of the log file that is saved to the disk. When the log file reaches the specified maximum size, the current log file is saved and a new active log file is started. The default maximum log file size is 10 MB and the maximum log file size allowed is 10 GB.
Roll log time	At the specified time of day, the current log file is saved and a new active log file is started.
Roll Log Frequency	The number of times the current log should be saved and a new active log started: each minute, hour, or day (as selected in the Unit drop down list).
Unit	The unit of time that corresponds to the specified Roll Log Frequency: minute, hour, or day.
Roll log day	The day of the week when the log should be saved and a new log started. At midnight on the specified day the current log file is saved and a new active log file is started.
Roll log policy	The policy to follow for saving the current log and starting a new active log. Overwritten deletes the oldest log entry when the disk is full. Block traffic stops all network traffic when the disk is full. Do not log stops logging messages when the disk is full.
Level	The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select Error, the unit logs Error, Critical, Alert and Emergency level messages. See <a href="#">Table 31, "Logging severity levels," on page 342</a> .

## Log file upload settings

Upload When Rolling	Select to upload log files to an FTP server whenever a log file rolls. Configure settings for the FTP server and select the type of log files to upload.
Upload Server IP	Enter the IP address of the FTP server to which to upload the log files.
Port	Enter the port number used by the FTP server. The default port is 21, which is the standard FTP port.
Username	Enter the user name required to connect to the FTP server.
Password	Enter the password required to connect to the FTP server.
Remote Directory	Enter the name of the path on the FTP server into which to transfer the log files. If you do not specify a remote directory, the log files are uploaded to the root directory of the FTP server.
Log files to upload	Select the log files to upload to the FTP server. You can upload the Traffic Log file, Event Log file, Antivirus Log file, Web Filter Log file, Attack Log file, Spam Filter Log file, and Content Archive file.

### To configure log file uploading

- 1 Select the blue arrow to expand Log file upload settings.
- 2 Select Upload When Rolling.
- 3 Enter the IP address of the logging server.
- 4 Enter the port number on the logging server. The default is 21 (FTP).
- 5 Enter the Username and Password required on the logging server.
- 6 Enter the remote directory in which to save the log files.
- 7 Select the types of log files to upload.
- 8 Select Apply.

### Memory settings

**Level** The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select Error, the unit logs Error, Critical, Alert and Emergency level messages. See [Table 31, "Logging severity levels," on page 342.](#)

### Syslog settings

**Name/IP** The domain name or IP address of the syslog server that stores the logs.

**Port** The port number for communication with the syslog server.

**Level** The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select Error, the unit logs Error, Critical, Alert and Emergency level messages. See [Table 31, "Logging severity levels," on page 342.](#)

**Facility** Facility indicates the source of a log message. By default, FortiGate reports Facility as local7. You might want to change Facility to distinguish log messages from different FortiGate units.

**Enable CSV Format** If you enable CSV format, the FortiGate unit produces the log in Comma Separated Value (CSV) format. If you do not enable CSV format the FortiGate unit produces plain text files.

### WebTrends settings

**Name/IP** The domain name or IP address of the WebTrends server that stores the logs.

**Level** The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select Error, the unit logs Error, Critical, Alert and Emergency level messages. See [Table 31, "Logging severity levels," on page 342.](#)



**Note:** To record traffic log messages, you must set the logging severity level to Notification when configuring the logging location. Traffic log messages do not generally have a severity level higher than Notification.  
Also, you must enable traffic logging for specific interfaces or firewall policies.

## Alert E-mail options

In Alert E-mail options you specify the mail server and recipients for email messages and you specify the severity level and frequency of the messages.

**Figure 184:Alert email configuration settings**

<b>Authentication Enable</b>	Select the Authentication Enable check box to enable SMTP authentication.
<b>SMTP Server</b>	The name/address of the SMTP server for email.
<b>SMTP User</b>	The SMTP user name.
<b>Password</b>	The SMTP password.
<b>Email To</b>	Enter one to three email recipients for alert email.
<b>Test</b>	Select Test to send a test alert email to the configured recipients.
<b>Level</b>	The FortiGate unit sends alert email for all messages at and above the logging severity level you select.
<b>Emergency</b>	The interval to wait before sending an alert e-mail for emergency level log messages.
<b>Alert</b>	The interval to wait before sending an alert e-mail for alert level log messages.
<b>Critical</b>	The interval to wait before sending an alert e-mail for critical level log messages.
<b>Error</b>	The interval to wait before sending an alert e-mail for error level log messages.
<b>Warning</b>	The interval to wait before sending an alert e-mail for warning level log messages.
<b>Notification</b>	The interval to wait before sending an alert e-mail for notification level log messages.
<b>Information</b>	The interval to wait before sending an alert e-mail for information level log messages.
<b>Apply</b>	Select Apply to activate any additions or changes to configuration.





**Note:** If more than one log message is collected before an interval is reached, the messages are combined and sent out as one alert email.

You can select specific events to trigger alert email in Log Filter, described in [“Log filter options” on page 345](#).

### To configure alert email



**Note:** Before configuring alert email make sure you configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server.

- 1 Go to **Log&Report > Alert E-mail**.
- 2 Select Enable to enable SMTP Authentication if required.
- 3 Configure the SMTP server, user, and password information if required.
- 4 Type up to three email addresses, one per Email To field.
- 5 Configure the time limit in which to send email for each logging severity level.
- 6 Select the logging severity level for which you want to send alert email.
- 7 Select Apply.

## Log filter options

For each logging location you enable, you can create a customized log filter based on the log types described in the following sections.



**Note:** Log locations must be enabled in Log Setting to be available for selection in the Log Filter.

Figure 185: Example traffic and event log filter settings

Log Filter							
	Check All	Fortilog	Disk	Memory	Syslog	WebTrends	Alert E-mail
▶ <b>Traffic Log</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ <b>Event Log</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▼ <b>Anti-virus Log</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Virus infected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Filename blocked	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
File oversized	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ <b>Web Filter Log</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Content block	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
URL block	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
URL exempt	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Blocked category ratings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitored category ratings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Category rating errors	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ <b>Attack Log</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Attack Signature	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Attack Anomaly	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▼ <b>Spam Filter Log</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SMTP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
POP3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
IMAP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ <b>Content Log</b>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Traffic log

The Traffic Log records all the traffic to and through the FortiGate interfaces. You can configure logging for traffic controlled by firewall policies and for traffic between any source and destination addresses. You can also apply global settings, such as session or packet log. You can apply the following filters:

- Policy allowed traffic**      The FortiGate unit logs all traffic that is allowed according to the firewall policy settings.
- Policy violation traffic**      The FortiGate unit logs all traffic that violates the firewall policy settings.



**Note:** You can enable traffic logging for specific interfaces or firewall policies. See [“Enabling traffic logging”](#) on page 348 for more information.

## Event log

The Event Log records management and activity events, such as when a configuration has changed or a routing gateway has been added. You can apply the following filters:

<b>System Activity event</b>	The FortiGate unit logs all system-related events, such as ping server failure and gateway status.
<b>IPSec negotiation event</b>	The FortiGate unit logs all IPSec negotiation events, such as progress and error reports.
<b>DHCP service event</b>	The FortiGate unit logs all DHCP-events, such as the request and response log.
<b>L2TP/PPTP/PPPoE service event</b>	The FortiGate unit logs all protocol-related events, such as manager and socket creation processes.
<b>Admin event</b>	The FortiGate unit logs all administrative events, such as user logins, resets, and configuration updates.
<b>HA activity event</b>	The FortiGate unit logs all high availability events, such as link, member, and state information.
<b>Firewall authentication event</b>	The FortiGate unit logs all firewall-related events, such as user authentication.
<b>Pattern update event</b>	The FortiGate unit logs all pattern update events, such as antivirus and IPS pattern updates and update failures.

### Anti-virus log

The Anti-virus Log records virus incidents in Web, FTP, and email traffic, such as when the FortiGate unit detects an infected file, blocks a file type, or blocks an oversized file or email. You can apply the following filters:

<b>Virus infected</b>	The FortiGate unit logs all virus infections.
<b>Filename blocked</b>	The FortiGate unit logs all instances of blocked files.
<b>File oversized</b>	The FortiGate unit logs all instances of oversized files.

### Web filter log

The Web Filter Log records HTTP content blocks, URL blocks, and URL exempt events. You can apply the following filters:

<b>Content block</b>	The FortiGate unit logs all instances of blocked content (specified in the banned words list).
<b>URL block</b>	The FortiGate unit logs all instances of blocked URLs (specified in the URL block list).
<b>URL exempt</b>	The FortiGate unit logs all instances of allowed URLs (specified in the URL exempt list).
<b>Blocked category ratings</b>	The FortiGate unit logs all access attempts to URLs blocked because of web category filtering settings.
<b>Monitored category ratings</b>	The FortiGate unit logs all access attempts to URLs monitored because of web category filtering settings.
<b>Category rating errors</b>	The FortiGate unit logs all instances of web category filtering rating errors.

## Attack log

The Attack Log records attacks detected and prevented by the FortiGate unit. You can apply the following filters:

<b>Attack Signature</b>	The FortiGate unit logs all detected and prevented attacks based on the attack signature, and the action taken by the FortiGate unit.
<b>Attack Anomaly</b>	The FortiGate unit logs all detected and prevented attacks based on unknown or suspicious traffic patterns, and the action taken by the FortiGate unit.

## Spam filter log

The Spam Filter Log records blocking of address patterns and content in IMAP and POP3 traffic. You can apply the following filters:

<b>SMTP</b>	The FortiGate unit logs all instances of blocked email in SMTP traffic.
<b>POP3</b>	The FortiGate unit logs all instances of blocked email in POP3 traffic.
<b>IMAP</b>	The FortiGate unit logs all instances of blocked email in IMAP traffic.

## Configuring log filters

Configure log filters for each location to which you are saving logs.

### To configure log filters

- 1 Go to **Log&Report > Log Config > Log Filter**.
- 2 Enable the logging type for each location to which you want to log messages.
- 3 Select the specific log sub-types to log for each location.
- 4 Select Apply.

## Enabling traffic logging

### To enable traffic logging for an interface or VLAN subinterface

You can enable traffic logging for an interface or VLAN subinterface. All connections to and through the interface are recorded in the traffic log.



**Note:** To record traffic log messages you must set the logging severity level to Notification when configuring the logging location. Traffic log messages do not generally have a severity level higher than Notification.

- 1 Go to **System > Network > Interface**.
- 2 Select the Edit icon for an interface.
- 3 Select Log.
- 4 Select OK.
- 5 Repeat steps 1 through 4 for each interface for which you want to enable logging.
- 6 Make sure you enable traffic logs for a logging location and set the logging severity level to Notification or lower.

### To enable traffic logging for a firewall policy

You can enable traffic logging for a firewall policy. All connections accepted by the firewall policy are recorded in the traffic log.

- 1 Go to **Firewall > Policy**.
- 2 Select the Edit icon for a policy.
- 3 Select Log Traffic.
- 4 Select OK.
- 5 Make sure you enable traffic log under Log Filter for a logging location and set the logging severity level to Notification or lower.

## Log access

Log Access provides access to log messages saved to the FortiGate disk or to the memory buffer. You can delete, view, search, and navigate logs.



**Note:** FortiGate units do not save some types of logs to memory. You can view these log messages with Log Access only if your FortiGate unit contains a hard disk drive.

On its disk, the FortiGate unit saves log messages in files. To view log messages, you must first select the file to open. You can also delete a file, clear (remove the log messages from) a file, or download a file in either plain text or CSV format.

You can view the log messages in a memory buffer simply by accessing the buffer. You cannot delete or download log messages from the memory buffer.













This section describes:

- [Disk log file access](#)
- [Viewing log messages](#)
- [Searching log messages](#)

### Disk log file access

You can view, navigate, and download logs saved to the FortiGate disk.

**Figure 186: Sample list of logs stored on the FortiGate disk**

Type:	File name	Size	Last access time	
Disk	elog	6656	Tue Jan 13 08:44:17 2004	  
	elog.1	9216	Thu Jan 8 15:58:47 2004	  
	elog.2	12800	Tue Dec 23 12:45:52 2003	  
	elog.3	1414656	Mon Dec 15 10:05:32 2003	  

The following table describes the column headings and the icons you can use to view and manage the log files when accessing logs saved to the disk.

<b>Type</b>	Select the log location for which you want to view logs: disk or memory. For some types of logs only disk storage is available.
<b>File name</b>	The name(s) of the log file(s) of that type stored to disk.
<b>Size</b>	The size of the log file in bytes.
<b>Last access time</b>	The day of the week, month, day, time, and year the log file was last added to by the FortiGate unit.  Delete icon. Delete the entire log file. You can't delete the current log file. Clear log icon. Delete the log entries from the log file (but not the file). Download icon. Download the log as a text or CSV file. View icon. Display the log file through the web-based manager.

#### **To access log files on the FortiGate disk**

- 1 Go to **Log&Report > Log Access**.
- 2 Select the log type you wish to access.
- 3 Select Disk from the Type list.
- 4 You can clear or delete, download, or view the log files by selecting the corresponding icon.

#### **To download log files from the FortiGate disk**

When downloading a log file, you can save the log in plain text or CSV format.

- 1 Go to **Log&Report > Log Access**.
- 2 Select the log type you wish to access.
- 3 Select Disk from the Type list.
- 4 Select the Download icon for the file you wish to download.
- 5 Select Download file in normal or CSV format.
- 6 Select Open to view the log file or Save to save the log file to your computer.

#### **To view and search log messages on the FortiGate disk**

- 1 Go to **Log&Report > Log Access**.
- 2 Select the log type you wish to access.
- 3 Select Disk from the Type list.
- 4 Select the View icon for the disk file you want to display.

For detailed information about searching logs, see [“Searching log messages” on page 353](#).

## Viewing log messages

You can view and navigate log messages saved to FortiGate hard disk drives or to the memory buffer.

**Figure 187: Viewing log messages**

#	Date	Time	Level	User Interface	Action	Message
1	2004-07-27	12:01:33	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
2	2004-07-27	12:01:31	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
3	2004-07-27	11:41:59	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
4	2004-07-27	11:41:57	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
5	2004-07-27	11:41:56	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
6	2004-07-27	11:29:06	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
7	2004-07-27	11:29:03	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
8	2004-07-27	11:29:03	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
9	2004-07-27	11:21:37	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
10	2004-07-27	11:21:34	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
11	2004-07-27	11:12:34	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
12	2004-07-27	11:12:31	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
13	2004-07-27	11:01:33	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)

The following table describes the features and icons you can use to navigate and search the logs when viewing logs through the web-based manager.

<b>Type</b>	Select the log location for which you want to view logs: disk or memory.
	Go to previous page icon. View to the previous page in the log file.
	Go to next page icon. View to the next page in the log file.
<b>View per page</b>	Select the number of log messages displayed on each page.
<b>Line: /</b>	Type the line number of the first line you want to display. The number following the slash ("/") is the total number of lines in the log.
<b>Search</b>	Type a search word and select Go.
<b>Advanced Search</b>	Select to search log messages by date, time and keywords.
	Column settings button. Select to choose columns for log display.
<b>Raw or Formatted</b>	Select Raw to switch to an unformatted log message display. Select Formatted to switch to a log message display organized into columns.

### To view log messages in the FortiGate memory buffer

- 1 Go to **Log&Report > Log Access**.
  - 2 Select the log type you wish to view.
  - 3 Select Memory from the Type list.
- The log messages are displayed.

You can change the displayed columns or see the raw log messages, go to the previous or next log page, or search the log by selecting the corresponding icon.

### To view log messages in FortiGate disk drive files

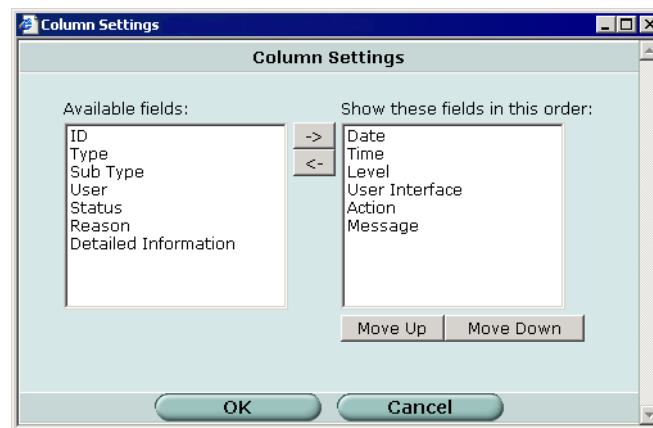
- 1 Go to **Log&Report > Log Access**.
- 2 Select the log type you wish to view.

- 3 Select Disk from the Type list.  
The log files are displayed.
- 4 Select the View icon for the log file you want to open.  
The log messages are displayed.  
You can change the displayed columns or see the raw log messages, go to the previous or next log page, or search the log by selecting the corresponding icon.

### Choosing columns

You can customize your log messages display using the Column Settings window. The column settings apply only when the formatted (not raw) display is selected.

**Figure 188:Column settings for viewing log messages**



**Available fields** The fields that you can add to the log message display.

-> Right arrow button. Select to move selected fields from Available fields list to Show these fields list.

<- Left arrow button. Select to move selected fields from the Show these fields list to the Available fields list.

**Show these fields in this order** The fields that are displayed as columns in the log messages list. The fields are listed in order with the first column at the top of the list.

**Move up** Move selected field up one position in the Show these fields list.

**Move down** Move selected field down one position in the Show these fields list.

The Detailed Information column provides the entire raw log entry and is not needed unless the log contains information not available in any of the other, more specific columns.

### To change the columns in the log message display

- 1 While viewing log messages, select the Column Settings icon.  
The Column Settings window opens.
- 2 To add fields, select them in the Available fields list and select the right arrow button.



- 3 To remove fields, select them in the Show these fields list and select the left arrow button.
- 4 To change the position of a column, select the field in the Show these fields list and then select Move Up or Move Down as necessary.
- 5 Select OK.

## Searching log messages

There are two ways to search log messages: a simple keyword search or an advanced search that enables you to use multiple keywords and specify a time range.

### To perform a simple keyword search

- 1 Display the log messages you want to search. For more information, see [“Viewing log messages” on page 351](#).
- 2 In the Search field, type a keyword and select Go.  
The log message list shows only the logs containing the keyword.

### To perform an advanced search

- 1 Display the log messages you want to search. For more information, see [“Viewing log messages” on page 351](#).
- 2 Select Advanced Search.  
The Log Search window is displayed.

**Figure 189: Search for log messages**

- 3 If you want to search for log messages in a particular date range, select the From and To dates.
- 4 Select one of the following options:
 

all of the following	The message must contain all of the keywords
any of the following	The message must contain at least one of the keywords
none of the following	The message must contain none of the keywords
- 5 In the Keywords field, type the keywords for the search.
- 6 Select OK.  
The log message list shows only the logs that meet your log search criteria.

## CLI configuration

This guide only covers Command Line Interface (CLI) commands and command keywords that are not represented in the web-based manager. For complete descriptions of working with CLI commands see the *FortiGate CLI Reference Guide*.

### fortilog setting



**Note:** The command keywords for `fortilog setting` that are not represented in the web-based manager are `localid` and `psksecret`.

Use this command to configure log settings for logging to a FortiLog unit.

The FortiLog unit is a log analyzer and manager that can combine the log information from various FortiGate units.

#### Command syntax pattern

```
config log fortilog setting
  set <keyword> <variable>

config log fortilog setting
  unset <keyword>

get log fortilog setting

show log fortilog setting
```

#### log fortilog setting command keywords and variables

Keywords and variables	Description	Default	Availability
<code>encrypt</code> {enable   disable}	Enter enable to enable encrypted communication with the FortiLog unit.	disable	All models.
<code>localid &lt;str_id&gt;</code>	Enter the local ID for an IPsec VPN tunnel to a FortiLog unit. You can create an IPsec VPN tunnel if one or more FortiGate units are sending log messages to a FortiLog unit across the Internet. Using an IPsec VPN tunnel means that all log messages sent by the FortiGate are encrypted and secure.	No default.	All models.
<code>psksecret</code> <str_psk>	Enter the pre-shared key for the IPsec VPN tunnel to a FortiLog unit. You can create an IPsec VPN tunnel if one or more FortiGate units are sending log messages to a FortiLog unit across the Internet. Using an IPsec VPN tunnel means that all log messages sent by the FortiGate are encrypted and secure.	No default.	All models.
<code>server</code> <address_ipv4>	Enter the IP address of the FortiLog unit.	No default.	All models.
<code>status</code> {disable   enable}	Enter enable to enable logging to a FortiLog unit.	disable	All models.



**Note:** The IPsec VPN settings for the FortiGate unit must match the VPN settings on the FortiLog unit.

## Example

This example shows how to enable logging to a FortiLog unit, set the FortiLog IP address, add a local ID, and add a pre-shared key for an IPSec VPN tunnel.

```
config log fortilog setting
  set status enable
  set server 192.168.100.1
  set localid net_host_c
  set psksecret J7fram54AhTWmoF5
end
```

This example shows how to display the log setting for logging to a FortiLog unit.

```
get log fortilog setting
```

This example shows how to display the configuration for logging to a FortiLog unit.

```
show log fortilog setting
```

If the `show` command returns you to the prompt, the settings are at default.

## syslogd setting



**Note:** The only command keyword for `syslogd setting` that is not represented in the web-based manager is the `facility` keyword.

Use this command to configure log settings for logging to a remote syslog server.

You can configure the FortiGate unit to send logs to a remote computer running a syslog server.

## Command syntax pattern

```
config log syslogd setting
  set <keyword> <variable>

config log syslogd setting
  unset <keyword>

get log syslogd setting

show log syslogd setting
```

## log syslogd setting command keywords and variables

Keywords and variables	Description	Default	Availability
csv {disable   enable}	Enter enable to enable the FortiGate unit to produce the log in Comma Separated Value (CSV) format. If you do not enable CSV format the FortiGate unit produces plain text files.	disable	All models.

**log syslogd setting command keywords and variables**

Keywords and variables	Description	Default	Availability
facility {alert   audit   auth   authpriv   clock   cron   daemon   ftp   kernel   local0   local1   local2   local3   local4   local5   local6   local7   lpr   mail   news   ntp   syslog   user   uucp}	Enter the facility type. Also known as message category, facility indicates from which part of the system a log message originated. Facility can also be used to route messages to different files. Facility types are described in <a href="#">Table 32</a> .	local7	All models.
port <port_integer>	Enter the port number for communication with the syslog server.	514	All models.
server <address_ipv4>	Enter the IP address of the syslog server that stores the logs.	No default.	All models.
status {disable   enable}	Enter <i>enable</i> to enable logging to a remote syslog server.	disable	All models.

**Table 32: Facility types**

Facility type	Description
alert	
audit	
auth	security/authorization messages
authpriv	security/authorization messages (private)
clock	clock daemon
cron	cron daemon performing scheduled commands
daemon	system daemons running background system processes
ftp	File Transfer Protocol (FTP) daemon
kernel	kernel messages
local0 – local7	reserved for local use
lpr	line printer subsystem
mail	email system
news	network news subsystem
ntp	Network Time Protocol (NTP) daemon
syslog	messages generated internally by the syslog daemon

## Example

This example shows how to enable logging to a remote syslog server, configure an IP address and port for the server, and set the facility type to user.

```
config log syslogd setting
    set status enable
    set server 220.210.200.190
    set port 601
    set facility user
end
```

This example shows how to display the log setting for logging to a remote syslog server.

```
get log syslogd setting
```

This example shows how to display the configuration for logging to a remote syslog server.

```
show log syslogd setting
```

If the `show` command returns you to the prompt, the settings are at default.



# FortiGuard categories

FortiGuard is a web filtering solution provided by Fortinet. FortiGuard sorts thousands of Web pages into a wide variety of categories that users can allow, block, or monitor. The FortiGate unit accesses the nearest FortiGuard server to determine the category of a requested Web page and then follows the policy configured for that user or interface.

Please see [“Category block” on page 317](#) for more information about how FortiGuard works and how to configure it.

[Table 33](#) describes each FortiGuard category.

**Table 33: FortiGuard categories**

Category name	Description
<b>Potentially Liable</b>	
1. Abused Drugs	Sites that promote or provide information about the use of prohibited drugs, or the abuse or unsanctioned use of controlled or regulated drugs; also, paraphernalia associated with such use or abuse, and sites that provide information about or promote the cultivation, preparation, or use of marijuana.
2. Cult or Occult	Sites that provide information about or promote religions not specified in Traditional Religions or other unconventional, cultic, or folkloric beliefs and practices. Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, satanic or supernatural beings.
3. Hacking	Sites that provide information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases. Proxy Avoidance -- sites that provide information about how to bypass proxy server features or to gain access to URLs in any way that bypasses the proxy server. URL Translation Sites -- sites that offer online translation of URLs. These sites access the URL to be translated in a way that bypasses the proxy server, potentially allowing unauthorized access.
4. Illegal or Questionable	Sites that provide instruction in or promote nonviolent crime or unethical or dishonest behavior or the avoidance of prosecution.

Table 33: FortiGuard categories

Category name	Description
5. Racism or Hate	Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.
6. Violence	Sites that feature or promote violence or bodily harm, including self-inflicted harm; or that gratuitously display images of death, gore, or injury; or that feature images or descriptions that are grotesque or frightening and of no redeeming value.
<b>Objectionable or Controversial</b>	
7. Abortion	Sites with neutral or balanced presentation of the issue. Pro-Choice -- Sites that provide information about or are sponsored by organizations that support legal abortion or that offer support or encouragement to those seeking the procedure. Pro-Life -- Sites that provide information about or are sponsored by organizations that oppose legal abortion or that seek increased restriction of abortion.
8. Adult Materials	Sites that display full or partial nudity in a sexual context, but not sexual activity; erotica; sexual paraphernalia; sex-oriented businesses as clubs, nightclubs, escort services; and sites supporting online purchase of such goods and services. Sex Education -- Sites that offer information about sex and sexuality, with no pornographic intent.
9. Advocacy Groups	Sites that promote change or reform in public policy, public opinion, social practice, economic activities and relationships.
10. Alcohol and Tobacco	Sites that provide information about, promote, or support the sale of alcoholic beverages or tobacco products or associated paraphernalia
11. Gambling	Sites that provide information about or promote gambling or support online gambling, involving a risk of losing money.
12. Militancy and Extremist	Sites that offer information about or promote or are sponsored by groups advocating anti government beliefs or action.
13. Nudity	Lingerie and Swimsuit -- Sites that offer images of models in suggestive but not lewd costume, with semi nudity permitted. Includes classic 'cheese-cake,' calendar, and pin-up art and photography. Includes also sites offering lingerie or swimwear for sale. Nudity -- Sites that offer depictions of nude or semi nude human forms, singly or in groups, not overtly sexual in intent or effect
14. Pornography	Sites that depict or graphically describe sexual acts or activity, including exhibitionism; also sites offering direct links to such sites.
15. Tasteless	Sites with content that is gratuitously offensive or shocking, but not violent or frightening. Includes sites devoted in part or whole to scatology and similar topics or to improper language, humor, or behavior.



Table 33: FortiGuard categories

Category name	Description
16. Weapons	Sites that provide information about, promote, or support the sale of weapons and related items. Sport Hunting and Gun Clubs -- Sites that provide information about or directories of gun clubs and similar groups, including war-game and paintball facilities.
<b>Potentially Non-productive</b>	
17. Advertisement	Sites that provide advertising graphics or other ad content files.
18. Brokerage and Trading	Sites that support active trading of securities and management of investments.
19. Freeware and Software Download	Sites whose primary function is to provide freeware and software downloads.
20. Games	Sites that provide information about or promote electronic games, video games, computer games, role-playing games, or online games. Includes sweepstakes and giveaways.
21. Internet Communication	Web Chat -- Sites that host Web chat services or that support or provide information about chat via HTTP or IRC. Instant Messaging -- Sites that enable instant messaging. Message Boards and Clubs -- Sites for online personal and business clubs, discussion groups, message boards, and list servers; includes 'blogs' and 'mail magazines.' Digital post cards - Sites for sending/viewing digital post cards.
22. Pay to Surf	Sites that pay users to view Web sites, advertisements, or email
23. Web-based Email	Sites that host Web-based email.
<b>Potentially Bandwidth Consuming</b>	
24. File Sharing and Storage	Peer-to-Peer File Sharing -- Sites that provide client software to enable peer-to-peer file sharing and transfer. Personal Network Storage and Backup -- Sites that store personal files on Internet servers for backup or exchange.
25. Streaming Media	MP3 -- Sites that support downloading of MP3 or other sound files or that serve as directories of such sites. Internet Radio and TV -- Sites whose primary purpose is to provide radio or TV programming on the Internet. Internet Telephony -- Sites that enable users to make telephone calls via the Internet or to obtain information or software for that purpose.
<b>Potentially Security Violating</b>	
26. Malicious Web Sites	Sites that contain code that may intentionally modify end-user systems without their consent and cause harm.
27. Spyware	Sites or pages that download software that, without the user's knowledge, generates http traffic (other than simple user identification and validation).

Table 33: FortiGuard categories

Category name	Description
<b>General Interest</b>	
28. Arts and Entertainment	Sites that provide information about or promote motion pictures, non-news radio and television, music and programming guides, books, humor, comics, movie theatres, galleries, artists or review on entertainment, and magazines.
29. Cultural Institutions	Sites sponsored by museums, galleries, theatres (but not movie theatres), libraries, and similar institutions; also, sites whose purpose is the display of artworks.
30. Education	Educational Institutions -- Sites sponsored by schools and other educational facilities, by non-academic research institutions, or that relate to educational events and activities. Educational Materials -- Sites that provide information about or that sell or provide curriculum materials or direct instruction; also, learned journals and similar publications. Sites for children
31. Financial Data and Services	Financial Data and Services -- Sites that offer news and quotations on stocks, bonds, and other investment vehicles, investment advice, but not online trading. Includes banks, credit unions, credit cards, and insurance.
32. Gay or Lesbian or Bisexual Interest	Gay or Lesbian or Bisexual Interest -- Sites that provide information about or cater to gay, lesbian, or bisexual lifestyles, including those that support online shopping, but excluding those that are sexually or issue-oriented.
33. Health	Sites that provide information or advice on personal health or medical services, procedures, or devices, but not drugs. Includes self-help groups.
34. Job Search	Sites that offer information about or support the seeking of employment or employees.
35. Medicine	Prescribed Medications -- Sites that provide information about approved drugs and their medical use. Supplements and Unregulated Compounds -- Sites that provide information about or promote the sale or use of chemicals not regulated by the FDA (such as naturally occurring compounds).
36. News and Media	Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines, or other media. Alternative Journals -- Online equivalents to supermarket tabloids and other fringe publications.
37. Personals and Dating	Personals and Dating -- Sites that assist users in establishing interpersonal relationships, excluding those intended to arrange for sexual encounters and excluding those of exclusively gay or lesbian or bisexual interest.
38. Political Organizations	Political Organizations -- Sites sponsored by or providing information about political parties and interest groups focused on elections or legislation.

**Table 33: FortiGuard categories**

Category name	Description
39. Reference Materials	Sites that offer reference-shelf content such as atlases, dictionaries, encyclopedias, formularies, white and yellow pages, and public statistical data.
40. Religion	Traditional Religions -- Sites that provide information about or promote Buddhism, Bahai, Christianity, Christian Science, Hinduism, Islam, Judaism, Mormonism, Shinto, and Sikhism, as well as atheism.
41. Search Engines and Portals	Search Engines and Portals -- Sites that support searching the Web, news groups, or indices or directories thereof.
42. Shopping and Auction	Sites that support the online purchase of consumer goods and services except: sexual materials, lingerie, swimwear, investments, medications, educational materials, computer software or hardware, alcohol, tobacco, travel, vehicles and parts, weapons. Internet Auctions -- Sites that support the offering and purchasing of goods between individuals. Real Estate -- Sites that provide information about renting, buying, selling, or financing residential real estate.
43. Social Organizations	Professional and Worker Organizations -- Sites sponsored by or that support or offer information about organizations devoted to professional advancement or workers interests. Service and Philanthropic Organizations -- Sites sponsored by or that support or offer information about organizations devoted to doing good as their primary activity. Social and Affiliation Organizations -- Sites sponsored by or that support or offer information about organizations devoted chiefly to socializing or common interests other than philanthropy or professional advancement.
44. Society and Lifestyles	Sites that provide information about matters of daily life, excluding entertainment, health, jobs, sex, and sports. Restaurants and Dining -- Sites that list, review, advertise, or promote food, dining, or catering services. Hobbies -- Sites that provide information about or promote private and largely sedentary pastimes, but not electronic, video, or online games. Personal Web Sites -- Sites published and maintained by individuals for their personal self-expression and ends.
45. Special Events	Sites devoted to a current event that requires separate categorization.
46. Sports	Sites that provide information about or promote sports, active games, and recreation.
47. Travel	Sites that provide information about or promote travel-related services and destinations.
48. Vehicles	Sites that provide information about or promote vehicles, including those that support online purchase of vehicles or parts.

Table 33: FortiGuard categories

Category name	Description
<b>Business Oriented</b>	
49. Business and Economy	Sites sponsored by or devoted to business firms, business associations, industry groups, or business in general.
50. Computer Security	Computer Security -- Sites that provide information about or free downloadable tools for computer security.
51. Government and Legal Organizations	Sites sponsored by branches, bureaus, or agencies of any level of government, except for the armed forces. Sites that discuss or explain laws of various government entities.
52. Information Technology	Sites sponsored by or providing information about computers, software, the Internet, and related business firms, including sites supporting the sale of hardware, software, peripherals, and services.
53. Military Organizations	Military -- Sites sponsored by branches or agencies of the armed services.
<b>Others</b>	
54. Dynamic Content	Dynamic Content -- URLs that are generated dynamically by a Web server.
55. Miscellaneous	Content Delivery Networks -- Commercial hosts that deliver content to subscribing Web sites. Image Servers -- Web servers whose primary function is to deliver images. Images (Media) -- URLs ending with image file names. Network Errors -- URLs with hosts that do not resolve to IP addresses. Private IP Addresses -- IP addresses defined in RFC 1918, 'Address Allocation for Private Intranets.
56. Web Hosting	Web Hosting -- Sites of organizations that provide hosting services, or top-level domain pages of Web communities.

# Glossary

**address:** An IP address (logical address) or the address of a physical interface (hardware address). An Ethernet address is sometimes called a MAC address. See also *IP address*.

**aggressive mode:** A way to establish a secure channel during IPSec phase 1 negotiations when the VPN peer uses its identity as part of the authentication process. See also *main mode*.

**AH, Authentication Header:** An IPSec security protocol. Fortinet IPSec uses ESP in tunnel mode, not AH. See *ESP*.

**ARP, Address Resolution Protocol:** A protocol that resolves a logical IP address to a physical Ethernet address.

**authentication:** A process whereby a server determines whether a client may establish a connection and access private resources.

**CA, Certificate Authority:** A company that issues digital certificates to validate the identity of a person or entity in an online exchange.

**CHAP, Challenge Handshake Authentication Protocol:** An authentication protocol supported by PPP. See also *PPP*.

**client:** An application that requires and requests services from a server.

**cluster:** A group of servers configured to act as a single fault-tolerant unit.

**connection:** A link between computers, applications, or processes that can be logical, physical, or both.

**decryption:** A method of decoding an encrypted file into its original state.

**DHCP, Dynamic Host Configuration Protocol:** An Internet protocol that assigns IP addresses to network clients, usually when the client connects to the Internet.

**Diffie-Hellman:** An algorithm for establishing a shared secret key over an insecure medium. See *Diffie-Hellman group*.

**Diffie-Hellman group:** FortiGate units support Diffie-Hellman groups 1, 2 and 5. The size of the modulus used to calculate the key varies according to the group:

- Group 1: 768-bit modulus
- Group 2: 1024-bit modulus
- Group 5: 1536-bit modulus

**digital certificate:** A digital document that guarantees the identity of a person or entity and is issued by a CA.

**DMZ, Demilitarized Zone:** An untrusted area of a private network, usually used to host Internet services without allowing unauthorized access to an internal (private) network. Typically, the DMZ contains servers accessible to Internet traffic, such as Web, FTP, SMTP, and DNS servers.

**DMZ interface:** The FortiGate interface that connects to a DMZ network.

**DNS, Domain Name System:** A service that converts symbolic node names to IP addresses. A domain name server (DNS server) implements the protocol.

**DoS, Denial-of-Service:** An attempt to disrupt a service by flooding the network with fake requests that consume network resources.

**DSL, Digital Subscriber Line:** A way to access the Internet at higher speeds using existing copper telephone lines. Users can maintain a continuous connection to the Internet and use the phone simultaneously.

**encapsulate:** Add a header to a packet to create a unit of transmission that matches the unit of transmission on a different network layer.

**encryption:** A method of encoding a file so that it cannot be understood. The information must be decrypted before it can be used.

**endpoint:** The IP address or port number that defines one end of a connection.

**ESP, Encapsulated Security Protocol:** An IPSec security protocol that provides encapsulation of encrypted data—IP packets are embedded in other IP packets so that the originating source and destination IP addresses cannot be seen on the Internet.

**Ethernet:** Can refer to the IEEE 802.3 signaling protocol, or an Ethernet controller (also known as a Media Access Controller or MAC).

**external interface:** The FortiGate interface that connects to the Internet.

**FTP, File Transfer Protocol:** A protocol used to transfer files between computers that have different operating systems.

**gateway:** A combination of hardware and layer-3 (network-layer) software that relays packets from one network to another.

**hash algorithm:** A procedure that renders a text message as a unique number.

**header:** The part of a packet that includes the source and destination address of the associated data. This addressing information is used to route packets.

**hop:** The segment of packet transmission that occurs between two routers. A packet may make several hops as it travels to its destination.

**host:** A network entity that has an IP address.

**HTTP, Hypertext Transmission Protocol:** The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

**HTTPS:** The secure HTML protocol for transmitting encrypted information to web servers using SSL. See also *SSL*.

**hub:** A device where communication links are brought together to exchange data between several computers.

**ICMP, Internet Control Message Protocol:** An IP message control protocol that supports error messages, test packets, and information messages related to IP. This protocol is used by the ping generator to send ICMP echo requests to a host.

**IKE, Internet Key Exchange:** A method of automatically exchanging IPsec authentication and encryption keys between two secure servers.

**IMAP, Internet Message Access Protocol:** An Internet email protocol that allows access to an email server from any IMAP-compatible browser.

**internal interface:** The FortiGate interface that connects to an internal (private) network.

**Internet:** The network that encompasses the world. As a generic term, it refers to any collection of interdependent networks.

**IP, Internet Protocol:** The component of TCP/IP that handles routing.

**IP address:** The point of attachment to a TCP/IP network. An IP address is a 32-bit quantity written in dotted decimal notation (four numbers separated by periods). See also *netmask*.

**IPSec, Internet Protocol Security:** A set of protocols that support secure exchange of packets at the IP layer. IPSec is most often used to support VPNs. See *VPN*.

**ISP, Internet Service Provider:** A company that provides customers with access to the Internet.

**KB, kilobyte:** A unit of storage (1 024 bytes).

**L2TP, Layer 2 Tunneling Protocol:** A security protocol that enables ISPs to establish VPN tunnels on behalf of dialup clients.

**LAN, Local Area Network:** A computer network that spans a relatively small area.

**Layer 2:** The data-link layer of the OSI model. Layer 2 is responsible for transmission, framing, and error control over a single link.

**Layer 3:** The network layer of the OSI model. Layer 3 is responsible for examining each network packet and sending them to the proper destination over the Internet.

**local:** The near end point (an IP address or port number) of a connection.

**MAC address, Media Access Control address:** A layer-2 hardware address that uniquely identifies a network node.

**main mode:** A way to hide the identities of VPN peers from passive eavesdroppers during IPsec phase 1 negotiations. See also *aggressive mode*.

**MB, Megabyte:** A unit of storage (1 048 576 bytes).

**MIB, Management Information Base:** A database of objects that can be monitored by an SNMP network manager.

**modem:** A device that converts digital signals into analog signals and back again for transmission over telephone lines.

**MTU, Maximum Transmission Unit:** The largest physical packet size, measured in bytes, that a network can transmit. Any packets larger than the MTU are divided into smaller packets before they are sent.

**NAT, Network Address Translation:** A way of routing IPv4 packets transparently. Using NAT, a router or FortiGate unit between a private and public network translates private IP addresses to public addresses and the other way around.

**netmask, network mask:** Also sometimes called subnet mask. A 32-bit quantity that indicates which bits of an IP address refer to the network portion.

**NTP, Network Time Protocol:** Used to synchronize the time of a computer to an NTP server. NTP provides accuracies to within tens of milliseconds across the Internet relative to coordinated universal time.

**OSI, Open Systems Interconnection:** A standard that defines network communication protocols using a seven-layer model.

**packet:** A piece of data transmitted over a packet-switched network. A packet contains a payload, the source and destination addresses, and a checksum. In IP networks, packets are often called datagrams. Packets are passed between the OSI data-link and network layers.

**PAP, Password Authentication Protocol:** An authentication protocol supported by PPP. See also *PPP*.

**ping, packet Internet grouper:** A utility for determining whether the device at a specific IP address is accessible. The utility sends a packet to the specified address and waits for a reply.

**POP3, Post Office Protocol:** A protocol used to transfer email from a mail server to a mail client across the Internet. Most email clients use POP.

**port:** The part of an interface on which application traffic is carried. By convention, the port number identifies the type of traffic. For example, port 80 is used for HTTP traffic.

**PPP, Point-to-Point Protocol:** A protocol for transmitting IP packets over serial point-to-point links (that is, across any DTE/DCE interface).

**PPPoE, PPP over Ethernet:** A protocol that specifies how to encapsulate PPP packets over Ethernet.

**PPTP, Point-to-Point Tunneling Protocol:** A security protocol that creates a VPN by encapsulating PPP packets.

**protocol:** A standard format for transmitting data. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

**RADIUS, Remote Authentication Dial-In User Service:** A user authentication and network-usage accounting system. When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

**remote:** The far end point (an IP address or port number) of a connection.

**replay detection:** A way to determine whether a replay attack is underway in an IPSec tunnel. A replay attack occurs when an unauthorized party intercepts a series of IPSec packets and changes them in an attempt to flood a tunnel or access a VPN.

**RFC, Request for Comments:** Internet Standards Committee documentation.

**RIP, Routing Information Protocol:** An Internet protocol for sharing routing information within an autonomous system.

**router:** A hardware device that connects computers on the Internet together and routes traffic between them. A router may connect a LAN and/or DMZ to the Internet.

**routing:** The process of determining which path to use for sending packets to a destination.

**routing table:** A list of possible paths that a packet can take to reach a destination.

**SA, Security Association:** SAs protect tunneled packets. They contain the information needed to create an IPSec VPN tunnel. An SA is uniquely identified by a security parameter index, an IP destination address, and a security protocol identifier. The Internet Security Association and Key Management Protocol (ISAKMP) is used to manage SAs.

**server:** An application that answers requests from clients. Used as a generic term for any device that provides services to the rest of the network such as printing, storage, and network access.

**SMTP, Simple Mail Transfer Protocol:** A protocol that supports email delivery services.

**SNMP, Simple Network Management Protocol:** A set of protocols for managing networks. SNMP agents store and return data about themselves to SNMP requesters.

**spam:** Unsolicited email.

**SSH, Secure Shell:** An application that enables users to log into a remote computer and run commands securely.

**SSL, Secure Sockets Layer:** An Internet security protocol that uses private and public encryption keys and certificates to keep transactions private.

**subnet, subnetwork:** A logical network comprising devices whose IP addresses have the same network prefix. For example, all devices having IP addresses in the 192.168.10.0/24 range can be accessed on the same subnet. See also *netmask*.

**TCP, Transmission Control Protocol:** One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets are delivered in the same order sent.

**trojan horse:** A harmful program that disguises itself as another program.

**UDP, User Datagram Protocol:** A connectionless protocol that runs on IP networks and is used primarily for broadcasting messages throughout the network.

**virus:** A computer program that replicates and spreads itself through computers or networks, usually with harmful intent.

**VPN, Virtual Private Network:** A secure logical network created from physically separate networks. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that data transmitted between VPN devices cannot be intercepted.

**worm:** A harmful program that replicates itself until it fills a computer or network, which can shut the system down.



# Index

## A

- abr-type 165
- access-list 176
- Action, Policy 267
- active sessions
  - HA monitor 95
- address 198
  - virtual IP 214
- Address Name, Policy 267
- administrator account
  - netmask 110, 111
  - trusted host 111
- advertise 172, 186
- alert email
  - enabling 345
  - options 344
- anomaly 284
  - list 284
- antivirus 289
- antivirus updates 121
  - through a proxy server 122
- area 179
- attack updates
  - scheduling 121
  - through a proxy server 122
- authentication 168, 174, 181
  - enabling 239
  - timeout 83
- Authentication Algorithm 254
- Authentication Algorithm, Manual Key 256
- Authentication Key, Manual Key 256
- Authentication Method 247
- authentication-key 174, 181
- Autokey Keep Alive 253

## B

- back up configuration 116
- bandwidth
  - guaranteed 195, 196
  - maximum 195, 196
- banned word
  - spam 333
- bindtoif 271

- border-routers 163
- browsing
  - the Internet through a VPN tunnel 253

## C

- CA certificates 264
- Certificate Name 248, 264
- CLI 18
  - upgrading the firmware 34, 36
- cluster
  - managing an HA cluster 94
- cluster ID
  - HA 95
- cluster members
  - HA 86
- command line interface 18
- Concentrator 252, 256
- Concentrator list 256
- Concentrator name 257
- Concentrator options 257
- Concentrator, Manual Key 256
- config distance 167
- config distribute-list 175
- config interface 180
- config limit 287
- config neighbor 177
- config network 179
- config offset-list 185
- config redistribute 184
- configuration
  - backup 116
  - reset to factory default 130
  - restore 116
- configuring
  - manual key IPsec VPN 254
- connecting a FortiGate HA cluster 91
- contact information
  - SNMP 98
- content block
  - web filter 311
- cost 178, 181
- CPU usage
  - HA monitor 95
- Create New 246, 251, 254, 257

csv 355  
custom TCP service 206, 207, 208  
custom UDP service 206, 207, 208  
customer service 23

## D

database 163  
    RIP 164  
database-filter-out 181  
database-overflow 165  
database-overflow-max-lsas 165  
database-overflow-time-to-recover 165  
date setting 81  
DDNS 56  
Dead Peer Detection 250  
dead-interval 174, 181  
debug log  
    back up 116  
    restore 116  
default heartbeat device configuration  
    HA 89  
default-cost 168  
default-information-metric 165  
default-information-metric-type 165  
default-information-originate 165  
default-information-route-map 165  
default-metric 166  
deny split tunneling 253  
destination IP address  
    example 267  
device 187  
device failover  
    HA 84  
DH Group 253  
DH Group, Phase 1 250  
DHCP-IPSec 253  
dialup VPN  
    monitor 258, 259  
direction 170  
Disk logging settings 342  
distance 166  
dpd-idlecleanup 269  
dpd-idleworry 269  
dpd-retrycount 270  
dpd-retryinterval 270  
dst 187, 258  
dst2 258  
dstaddr 271  
dstport 271  
Dynamic DNS 247  
    on network interface 52  
dynamic DNS  
    monitor 258, 259  
dynamic IP pool  
    IP pool 199, 234, 235, 237, 239  
dynamic port forwarding 215, 218

## E

Email address 330  
Enable perfect forward secrecy (PFS) 253  
Enable replay detection 253  
Encryption  
    for FortiLog unit 341  
Encryption Algorithm 247, 254  
Encryption Algorithm, Manual Key 255  
Encryption Key, Manual Key 255  
Exempt URL options 316  
expire  
    system status 32

## F

facility 356  
fail open 288  
failover  
    monitoring cluster units 96  
FDN  
    FortiProtect Distribution Network 118  
FDS  
    FortiProtect Distribution Server 118  
File block 290  
File block list 291  
firewall  
    authentication timeout 83  
    configuring 189  
    introduction 15  
    overview 189  
firewall policies for IPSec VPN  
    adding 266  
firewall policy  
    guaranteed bandwidth 195, 196  
    maximum bandwidth 195, 196  
firmware  
    installing 38  
    re-installing current version 38  
    reverting to an older version 38  
    upgrading to a new version 33  
    upgrading using the CLI 34, 36  
    upgrading using the web-base manager 33, 35  
Fortilog logging settings 341  
fortilog setting 354  
Fortinet customer service 23  
FortiProtect Distribution Network 118  
FortiProtect Distribution Server 118  
from IP  
    system status 32  
from port  
    system status 32, 58  
ftp 230

## G

gateway 187  
Gateway IP 246  
Gateway Name 246, 247

go  
 HA monitor 95  
 group ID  
 HA 86  
 grouping services 209  
 groups  
 user 239  
 guaranteed bandwidth 195, 196

## H

HA 84, 85  
 add a new unit to a functioning cluster 93  
 cluster ID 95  
 cluster members 86  
 configuration 85  
 configure a FortiGate unit for HA operation 90  
 configure weighted-round-robin weights 93  
 connect a FortiGate HA cluster 91  
 default heartbeat device configuration 89  
 device failover 84  
 group ID 86  
 heartbeat device IP addresses 89  
 heartbeat failover 84  
 introduction 18  
 link failover 84  
 manage individual cluster units 96  
 manage logs for individual cluster units 95  
 managing a cluster 94  
 mode 86  
 monitor 95  
 monitor cluster units for a failover 96  
 monitor priorities 90  
 override master 87  
 password 87  
 priorities of heartbeat device 88  
 schedule 88  
 status 95  
 unit priority 86  
 view the status of each cluster member 94  
 HA cluster  
 configuring 90  
 HA monitor  
 active sessions 95  
 CPU usage 95  
 intrusion detected 95  
 memory usage 95  
 monitor 95  
 network utilization 95  
 total bytes 95  
 total packets 95  
 up time 95  
 virus detected 95  
 heartbeat  
 failover 84  
 heartbeat device IP addresses  
 HA 89  
 hello-interval 174, 182

High Availability 85  
 high availability  
 introduction 18  
 http 230  
 HTTPS 18, 204  
 hub  
 HA schedule 88

## I

ICMP 205  
 idle timeout  
 web-based manager 83  
 IMAP 204  
 interface 163, 182  
 administrative status 48, 69  
 bringing down 54  
 bringing up 54  
 RIP 164  
 starting 54  
 Interface/Zone, Policy 267  
 Internet browsing  
 through a VPN tunnel 253  
 intrusion detected  
 HA monitor 95  
 IP 88  
 ip 178, 182, 273  
 IP Address 247  
 IP address 327  
 heartbeat device 89  
 IP address list 327, 329, 330, 332  
 IP address options 327, 329, 330, 332  
 IP pool  
 adding 219  
 IP port  
 HA schedule 88  
 IP Range/Subnet, Address 267  
 ipaddress 287  
 IPS 17, 277  
 anomaly 284  
 anomaly list 284  
 ipsec vip 272  
 IPSec VPN  
 authentication for user group 239  
 Internet browsing 253  
 monitor 258  
 ping generator 257  
 remote gateway 239  
 IPv6 71  
**K**  
 Keepalive Frequency 250  
 Key Size 264  
 Key Type 264  
 Keylife 250, 253

## L

- L2TP 239
  - configuring gateway 261
  - enabling 261
  - overview 261
- language
  - web-based manager 83
- Least-Connection
  - HA schedule 88
- Lifetime (sec/kb) 251
- link failover
  - HA 84
- list 170
- Local certificate list 262
- Local certificate options 263
- Local ID 250
- Local SPI, Manual Key 255
- Log & report 339
- Log file upload settings 342
- Log filter options 345
- Log settings 340
- Logging 349
- logging 19
- logs
  - managing for individual cluster units 95

## M

- manage cluster units
  - HA 96
- Managing digital certificates 262
- Manual Key 253
- manual key IPsec configuration
  - configuration steps 254
- Manual key list 254
- Manual key options 255
- matching
  - policy 190
- maximum bandwidth 195, 196
- md5-key 174, 182
- member 242
- Members 257
- memfilesizelimit 301, 303, 304, 306, 307
- Memory logging settings 343
- memory usage
  - HA monitor 95
- metric 185
- metric-type 185
- MIB
  - FortiGate 101
- MIME headers 331
- Mode 246, 247
- mode
  - HA 86
  - Transparent 16

- monitor
  - HA monitor 95
  - IPsec VPN 258
- monitor priorities
  - HA 90
- mtu 182
- MTU size 53
- mtu-ignore 182

## N

- NAT
  - introduction 16
  - push update 124
- NAT/Route mode
  - introduction 16
- natip 198
- Nat-traversal 250
- neighbor 163
- netmask
  - administrator account 110, 111
- network address translation
  - introduction 16
- network intrusion detection 17
- network utilization
  - HA monitor 95
- network-type 183
- next hop router 56
- none
  - HA schedule 88
- nssa-default-information-originate 168
- nssa-default-information-originate-metric 168
- nssa-default-information-originate-metric-typ 168
- nssa-redistribution 168
- nssa-translator-role 169
- NTP 205
- NTP server 82
  - setting system date and time 81

## O

- one-time schedule
  - creating 211, 212, 213
- options
  - changing system options 82
- OSPF 164
- out-interface 273
- override master
  - HA 87

## P

- P1 Proposal, Phase 1 249
- P2 Proposal, Phase 2 252
- passive-interface 166
- password
  - HA 87
- Pattern block options 315

peer 174  
Peer option 248  
Phase 1 246  
Phase 1 advanced options 249  
Phase 1 basic settings 247  
Phase 1 list 246  
Phase 2 250  
Phase 2 advanced options 252  
Phase 2 basic settings 251  
Phase 2 list 251  
ping generator  
  IPSec VPN 257  
policy  
  enabling authentication 239  
  guaranteed bandwidth 195, 196  
  IPSec VPN 266  
  matching 190  
  maximum bandwidth 195, 196  
policy routing 145  
poll-interval 178  
POP3 205  
port 301, 303, 304, 306, 307, 356  
port forward  
  dynamic 215  
port forwarding  
  virtual IP 215  
PPTP 239  
predefined services 203  
prefix 172, 179, 186  
Pre-shared Key 248  
Pre-shared key  
  for FortiLog unit 341  
priorities of heartbeat device  
  HA 88  
priority 178, 183  
profile 272  
  protection 222  
protection profile 222  
protocol 176, 271  
  service 204  
  system status 32  
Proxy ID Destination 259, 260  
Proxy ID Source 259, 260  
proxy server 122  
  push updates 122  
push update  
  configuring 123  
  external IP address changes 123  
  management IP address changes 124  
  through a NAT device 124  
  through a proxy server 122

## Q

Quarantine 292

Quarantine list 292  
Quick Mode Identities 253

## R

random  
  HA schedule 88  
RBL and ORDBL 328  
read & write access level  
  administrator account 81, 110, 115, 119, 126  
read only access level  
  administrator account 81, 110, 115  
recurring schedule  
  creating 213  
refresh every  
  HA monitor 95  
remote administration 57, 60  
Remote Gateway 247, 251, 252, 254  
Remote gateway 259, 260  
remote peer  
  manual key IPSec configuration 254  
Remote SPI, Manual Key 255  
reporting 19  
restarting 118  
restore configuration 116  
retransmit-interval 175, 183  
reverting  
  firmware to an older version 38  
rfc1583-compatible 166  
Round-Robin  
  HA schedule 88  
route 163  
routemap 185  
router  
  next hop 56  
router-id 166  
routing  
  configuring 61  
  policy 145

## S

schedule 211  
  automatic antivirus and attack definition updates 121  
  creating one-time 211, 212, 213  
  creating recurring 213  
  HA 88  
Schedule, Policy 267  
scheduled antivirus and attack updates 122  
scheduled updates  
  through a proxy server 122  
scheduling 121  
Script filter 321  
selector 272  
server 354, 356

- service 203
  - custom TCP 206, 207, 208
  - custom UDP 206, 207, 208
  - group 209
  - predefined 203
  - service name 204
  - user-defined TCP 206, 207, 208
  - user-defined UDP 206, 207, 208
- service ftp 302
- service http 300
- service imap 305
- service pop3 304
- service smtp 307
- Service, Policy 267
- set time 82
- shortcut 169
- Signature list 279
- Signatures 278
- single-source 272
- SMTP 206
- smtp 231
- SNMP
  - contact information 98
  - MIBs 101
  - traps 101
- source IP address
  - example 267
- spam
  - banned word 333
- Spam filter 323
- spf-timers 166
- split tunneling
  - deny 253
- src 258
- src2 258
- srcaddr 272
- srcport 272
- SSH 206
- SSL
  - service definition 204
- standalone mode 85
- static IP
  - monitor 258, 259
- static NAT virtual IP 215
- Status 251
- status 163, 183, 185, 258, 354, 356
  - HA monitor 95
  - interface 48, 69
- stub-type 169
- Subject Information 264
- substitute 172
- substitute-status 172
- syn interval 82
- synchronize with NTP server 82
- Syslog logging settings 343
- system configuration 81

- system date and time
  - setting 81
- system options
  - changing 82

## T

- tag 185, 186
- TCP
  - custom service 206, 207, 208
- technical support 23
- threshold 287
- time
  - setting 81
- time zone 82
- Timeout 251, 259, 260
- timeout
  - firewall authentication 83
  - idle 83
  - web-based manager 83
- to IP
  - system status 32
- to port
  - system status 32
- total bytes
  - HA monitor 95
- total packets
  - HA monitor 95
- Traffic Priority 195
- transmit-delay 175, 183
- Transparent mode 16
- traps
  - SNMP 101
- trusted host
  - administrator account 111
  - Administrators options 110
  - security issues 111
- Tunnel Name 251, 252
- type 169

## U

- UDP
  - custom service 206, 207, 208
- unit priority
  - HA 86
- up time
  - HA monitor 95
- update
  - push 123
- upgrade
  - firmware 33
- upgrading
  - firmware using the CLI 34, 36
  - firmware using the web-based manager 33, 35
- Uploading a local certificate 264
- URL block 312
- URL exempt 315

---

- URL options 313
- user groups
  - configuring 239
- User-defined signatures 282
- user-defined TCP services 206, 207, 208
- user-defined UDP services 206, 207, 208
- Username 259

## V

- virtual domain
  - properties 132
- virtual IP 214
  - dynamic port forwarding 218
  - port forwarding 215
  - static NAT 215
- virtual-links 163
- virus detected
  - HA monitor 95
- virus protection
  - worm protection 14
- VLAN
  - overview 62
- VLAN subinterface
  - bringing down 54
  - bringing up 54
  - starting 54
- VPN
  - introduction 17

- VPN certificates
  - restore 117
  - upload 117
- VPN Tunnel, Policy 267
- VPNs 245

## W

- web content filtering
  - introduction 14
- Web filter 309, 359
  - content block 311
- Web pattern block 314
- Web script filter options 322
- Web URL block list 313
- web-based manager
  - introduction 18
  - language 83
  - timeout 83
- WebTrends logging settings 343
- weighted round-robin
  - HA schedule 88
- weighted-round-robin
  - configuring weights 93

## X

- XAuth 250

