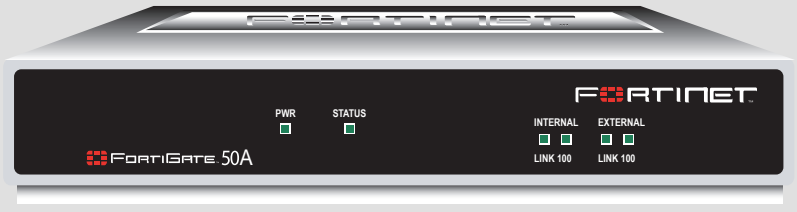
FortiGate 50A

Installation and Configuration Guide



FortiGate User Manual Volume 1

Version 2.50

29 February 2004

FortiGate-50A Installation and Configuration Guide
Version 2.50
29 February 2004

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**.

Table of Contents

Introduction

The FortiGate-50A Antivirus Firewall is an easy-to-deploy and easy-to-administer solution that delivers exceptional value and performance for small office and home office (SOHO) applications.

Your FortiGate-50A 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.

NAT/Route mode and Transparent mode

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

NAT/Route mode

In NAT/Route mode, the FortiGate-50A is installed as a privacy barrier between the internal network and the Internet. The firewall provides network address translation (NAT) to protect the internal private network. You can control whether firewall policies run in NAT mode or route mode. NAT mode policies route allowed connections between firewall interfaces, performing network address translation to hide addresses on the protected internal networks. Route mode policies route allowed connections between firewall interfaces without performing network address translation.

Transparent mode

Transparent Mode provides firewall protection to a pre-existing network with public addresses. The internal and external network interfaces of the FortiGate unit must be in the same subnet and the FortiGate unit can be inserted into your network at any point without the need to make any changes to your network.

Document conventions

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

- angle brackets `< >` to indicate variable keywords

  For example:

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

  You enter `restore config myfile.bak`

  `<xxx_str>` indicates an ASCII string variable keyword.

  `<xxx_integer>` indicates an integer variable keyword.

  `<xxx_ip>` indicates an IP address variable keyword.
- vertical bar and curly brackets `{|}` to separate alternative, mutually exclusive required keywords

  For example:

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

  You can enter `set system opmode nat` or `set system opmode transparent`
- square brackets `[ ]` to indicate that a keyword is optional

  For example:

  ```
  get firewall ipmacbinding [dhcpipmac]
  ```

  You can enter `get firewall ipmacbinding` or `get firewall ipmacbinding dhcpipmac`

Fortinet documentation

Information about FortiGate products is available from the following FortiGate User Manual volumes:

- *Volume 1: FortiGate Installation and Configuration Guide*

  Describes installation and basic configuration for the FortiGate unit. Also describes how to use FortiGate firewall policies to control traffic flow through the FortiGate unit and how to use firewall policies to apply antivirus protection, web content filtering, and email filtering to HTTP, FTP and email content passing through the FortiGate unit.
- *Volume 2: FortiGate VPN Guide*

  Contains in-depth information about FortiGate IPSec VPN using certificates, pre-shared keys and manual keys for encryption. Also contains basic configuration information for the Fortinet Remote VPN Client, detailed configuration information for FortiGate PPTP and L2TP VPN, and VPN configuration examples.
- *Volume 3: FortiGate Content Protection Guide*

  Describes how to configure antivirus protection, web content filtering, and email filtering to protect content as it passes through the FortiGate unit.
- *Volume 4: FortiGate NIDS Guide*

  Describes how to configure the FortiGate NIDS to detect and protect the FortiGate unit from network-based attacks.
- *Volume 5: FortiGate Logging and Message Reference Guide*

  Describes how to configure FortiGate logging and alert email. Also contains the FortiGate log message reference.
- *Volume 6: FortiGate CLI Reference Guide*

  Describes the FortiGate CLI and contains a reference to all FortiGate CLI commands.

The FortiGate online help also contains procedures for using the FortiGate web-based manager to configure and manage your FortiGate unit.

Comments on Fortinet technical documentation

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

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 FortiGate Antivirus Firewalls from http://support.fortinet.com and modify your registration information at any time.

Fortinet email support is available from the following addresses:

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 on Fortinet telephone support, see http://support.fortinet.com.

When requesting technical support, please provide the following information:

- Your name
- Company name
- Location
- Email address
- Telephone number
- FortiGate unit serial number
- FortiGate model
- FortiGate FortiOS firmware version
- Detailed description of the problem

Getting started

This chapter describes unpacking, setting up, and powering on a FortiGate Antivirus Firewall unit. When you have completed the procedures in this chapter, you can proceed to one of the following:

- If you are going to operate the FortiGate unit in NAT/Route mode, go to "NAT/Route mode installation" on page 33.
- If you are going to operate the FortiGate unit in Transparent mode, go to "Transparent mode installation" on page 41.

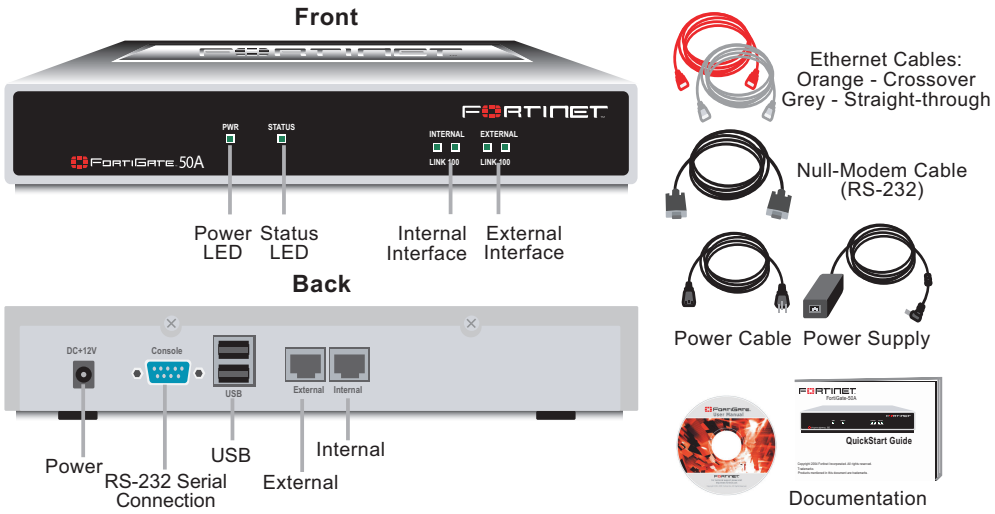
This chapter describes:

Package contents

The FortiGate-50A package contains the following items:

- the FortiGate-50A Antivirus Firewall
- one orange cross-over ethernet cable
- one gray regular ethernet cable
- one null-modem cable
- FortiGate-50A QuickStart Guide
- A CD containing the FortiGate user documentation
- one AC adapter

Figure 1: FortiGate-50A package contents



Mounting

The FortiGate-50A unit can be installed on any stable surface. Make sure that the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Dimensions

- 8.63 x 6.13 x 1.38 in. (21.9 x 15.6 x 3.5 cm)

Weight

- 1.5 lb. (0.68 kg)

Power requirements

- DC input voltage: 5 V
- DC input current: 3 A

Environmental specifications

- Operating temperature: 32 to 104°F (0 to 40°C)
- Storage temperature: -13 to 158°F (-25 to 70°C)
- Humidity: 5 to 95% non-condensing

Powering on

To power on the FortiGate-50A unit

1. Connect the AC adapter to the power connection at the back of the FortiGate-50 unit.
2. Connect the AC adapter to a power outlet.
   The FortiGate-50A starts up. The Power and Status lights light. The Status light flashes while the unit is starting up and turns off when the system is up and running.

Table 1: FortiGate-50A LED indicators

Power	Green	The FortiGate unit is powered on.
	Off	The FortiGate unit is powered off.
Status	Green	The FortiGate unit is starting.
	Off	The FortiGate unit is operating normally.
Link (Internal External)	Green	The correct cable is in use and the connected equipment has power.
	Flashing Green	Network activity at this interface.
	Off	No link established.
100 (Internal External)	Green	The interface is connected at 100 Mbps.

Connecting to the web-based manager

Use the following procedure to connect to the web-based manager for the first time. Configuration changes made with the web-based manager are effective immediately without resetting the firewall or interrupting service.

To connect to the web-based manager, you need:

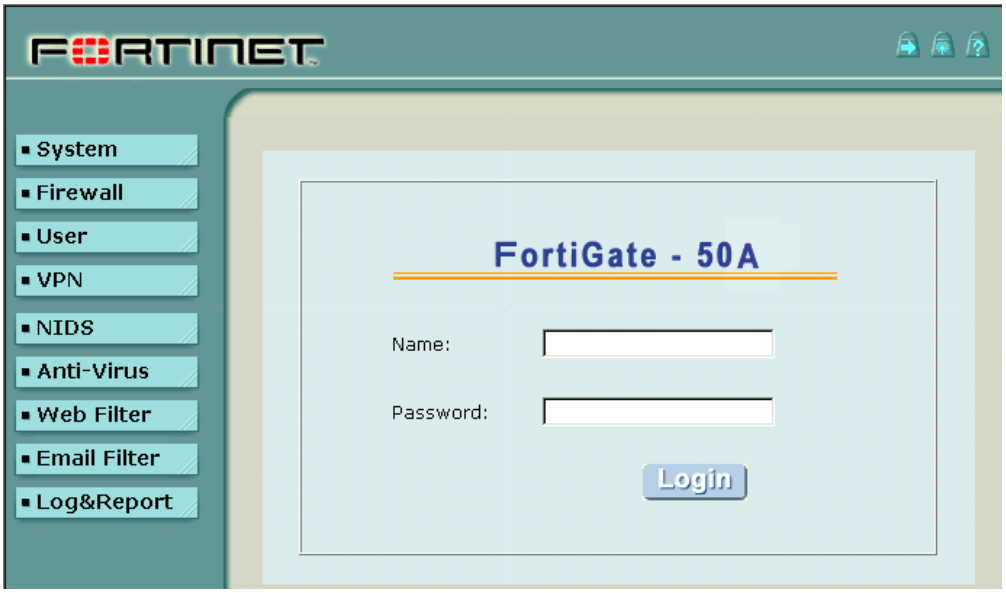
- a computer with an ethernet connection,
- Internet Explorer version 4.0 or higher,
- a crossover cable or an ethernet hub and two ethernet cables.

Note: You can use the web-based manager with recent versions of most popular web browsers. The web-based manager is fully supported for Internet Explorer version 4.0 or higher.

To connect to the web-based manager

1. Set the IP address of the computer with an ethernet connection to the static IP address 192.168.1.2 and a netmask of 255.255.255.0.
   You can also configure the management computer to obtain an IP address automatically using DHCP. The FortiGate DHCP server assigns the management computer an IP address in the range 192.168.1.1 to 192.168.1.254.
2. Using the crossover cable or the ethernet hub and cables, connect the internal interface of the FortiGate unit to the computer ethernet connection.
3. Start Internet Explorer and browse to the address https://192.168.1.99.
   The FortiGate login is displayed.
4. Type admin in the Name field and select Login.
   The Register Now window is displayed. Use the information in this window to register your FortiGate unit so that Fortinet can contact you for firmware updates. You must also register to receive updates to the FortiGate virus and attack definitions.

Figure 2: FortiGate login



Connecting to the command line interface (CLI)

As an alternative to the web-based manager, you can install and configure the FortiGate unit using the CLI. Configuration changes made with the CLI are effective immediately without resetting the firewall or interrupting service.

To connect to the FortiGate CLI, you need:

- a computer with an available communications port,
- the null modem cable included in your FortiGate package,
- terminal emulation software such as HyperTerminal for Windows.

Note: The following procedure describes how to connect to the CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the CLI

1. Connect the null modem cable to the communications port of your computer and to the FortiGate Console port.
2. Make sure that the FortiGate unit is powered on.
3. Start HyperTerminal, enter a name for the connection, and select OK.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the null modem cable and select OK.
5. Select the following port settings and select OK.

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

6. Press Enter to connect to the FortiGate CLI.
   The following prompt is displayed:
   ```
   FortiGate-50A login:
   ```
7. Type `admin` and press Enter twice.
   The following prompt is displayed:
   ```
   Type ? for a list of commands.
   ```
   For information about how to use the CLI, see the *FortiGate CLI Reference Guide*.

Factory default FortiGate configuration settings

The FortiGate unit is shipped with a factory default configuration. The default configuration allows you to connect to and use the FortiGate web-based manager to configure the FortiGate unit onto the network. To configure the FortiGate unit onto the network you add an administrator password, change network interface IP addresses, add DNS server IP addresses, and configure routing, if required.

If you plan to operate the FortiGate unit in Transparent mode, you can switch to Transparent mode from the factory default configuration and then configure the FortiGate unit onto the network in Transparent mode.

Once the network configuration is complete, you can perform additional configuration tasks such as setting system time, configuring virus and attack definition updates, and registering the FortiGate unit.

The factory default firewall configuration includes a single network address translation (NAT) policy that allows users on your internal network to connect to the external network, and stops users on the external network from connecting to the internal network. You can add more policies to provide more control of the network traffic passing through the FortiGate unit.

The factory default content profiles can be used to apply different levels of antivirus protection, web content filtering, and email filtering to the network traffic that is controlled by firewall policies.

Factory default DHCP configuration

When the FortiGate unit is first powered on, the external interface is configured to receive its IP address by connecting to a DHCP server. If your ISP provides IP addresses using DHCP, no other configuration is required for this interface.

The FortiGate unit can also function as a DHCP server for your internal network. You can configure the TCP/IP settings of the computers on your internal network to obtain an IP address automatically from the FortiGate unit DHCP server. For more information about the FortiGate DHCP server, see “Configuring DHCP services” on page 104.

Table 2: FortiGate DHCP Server default configuration

Enable DHCP	☑
Starting IP	192.168.1.1
Ending IP	192.168.1.254
Netmask	255.255.255.0
Lease Duration	604800 seconds
Default Route	192.168.1.99
Exclusion Range	192.168.1.99 - 192.168.1.99

Factory default NAT/Route mode network configuration

When the FortiGate unit is first powered on, it is running in NAT/Route mode and has the basic network configuration listed in Table 3. This configuration allows you to connect to the FortiGate unit web-based manager and establish the configuration required to connect the FortiGate unit to the network. In Table 3 HTTPS management access means you can connect to the web-based manager using this interface. Ping management access means this interface responds to ping requests.

Table 3: Factory default NAT/Route mode network configuration

Administrator account	User name: Password:	admin (none)
Internal interface	IP: Netmask: Management Access:	192.168.1.99 255.255.255.0 HTTPS, Ping
External interface	Addressing Mode: Management Access:	DHCP Ping

Factory default Transparent mode network configuration

If you switch the FortiGate unit to Transparent mode, it has the default network configuration listed in Table 4.

Table 4: Factory default Transparent mode network configuration

Administrator account	User name: Password:	admin (none)
Management IP	IP: Netmask:	10.10.10.1 255.255.255.0
DNS	Primary DNS Server: Secondary DNS Server:	207.194.200.1 207.194.200.129
Management access	Internal External	HTTPS, Ping Ping

Factory default firewall configuration

The factory default firewall configuration is the same in NAT/Route and Transparent mode.

Table 5: Factory default firewall configuration

Internal Address	Internal_All	IP: 0.0.0.0 Mask: 0.0.0.0	Represents all of the IP addresses on the internal network.
External Address	External_All	IP: 0.0.0.0 Mask: 0.0.0.0	Represents all of the IP addresses on the external network.

Table 5: Factory default firewall configuration (Continued)

Recurring Schedule	Always		The schedule is valid at all times. This means that the firewall policy is valid at all times.
Firewall Policy	**Int->Ext**		Firewall policy for connections from the internal network to the external network.
	Source	Internal_All	The policy source address. Internal_All means that the policy accepts connections from any internal IP address.
	Destination	External_All	The policy destination address. External_All means that the policy accepts connections with a destination address to any IP address on the external network.
	Schedule	Always	The policy schedule. Always means that the policy is valid at any time.
	Service	ANY	The policy service. ANY means that this policy processes connections for all services.
	Action	ACCEPT	The policy action. ACCEPT means that the policy allows connections.
	☑ **NAT**		NAT is selected for the NAT/Route mode default policy so that the policy applies network address translation to the traffic processed by the policy. NAT is not available for Transparent mode policies.
	☐ **Traffic Shaping**		Traffic shaping is not selected. The policy does not apply traffic shaping to the traffic controlled by the policy. You can select this option to control the maximum or minimum amount of bandwidth available to traffic processed by the policy.
	☐ **Authentication**		Authentication is not selected. Users do not have to authenticate with the firewall before connecting to their destination address. You can configure user groups and select this option to require users to authenticate with the firewall before they can connect through the firewall.
	☑ **Antivirus & Web Filter**		Antivirus & Web Filter is selected.
	Content Profile	Scan	The scan content profile is selected. The policy scans all HTTP, FTP, SMTP, POP3, and IMAP traffic for viruses. See “Scan content profile” on page 26 for more information about the scan content profile. You can select one of the other content profiles to apply different levels of content protection to traffic processed by this policy.
	☐ **Log Traffic**		Log Traffic is not selected. This policy does not record messages to the traffic log for the traffic processed by this policy. You can configure FortiGate logging and select Log Traffic to record all connections through the firewall that are accepted by this policy.

Factory default content profiles

You can use content profiles to apply different protection settings for content traffic that is controlled by firewall policies. You can use content profiles for:

- Antivirus protection of HTTP, FTP, IMAP, POP3, and SMTP network traffic
- Web content filtering for HTTP network traffic
- Email filtering for IMAP and POP3 network traffic
- Oversized file and email blocking for HTTP, FTP, POP3, SMTP, and IMAP network traffic
- Passing fragmented emails in IMAP, POP3, and SMTP email traffic

Using content profiles, you can build protection configurations that can be applied to different types of firewall policies. This allows you to 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 content profiles.

Content profiles can be added to NAT/Route mode and Transparent mode policies.

Strict content profile

Use the strict content profile to apply maximum content protection to HTTP, FTP, IMAP, POP3, and SMTP content traffic. You do not need to use the strict content profile under normal circumstances, but it is available if you have extreme problems with viruses and require maximum content screening protection.

Table 6: Strict content profile

Options	HTTP	FTP	IMAP	POP3	SMTP
Antivirus Scan	☑	☑	☑	☑	☑
File Block	☑	☑	☑	☑	☑
Web URL Block	☑				
Web Content Block	☑				
Web Script Filter	☑				
Web Exempt List	☑				
Email Block List			☑	☑	
Email Exempt List			☑	☑	
Email Content Block			☑	☑	
Oversized File/Email Block	block	block	block	block	block
Pass Fragmented Emails			☐	☐	☐

Scan content profile

Use the scan content profile to apply antivirus scanning to HTTP, FTP, IMAP, POP3, and SMTP content traffic.

Table 7: Scan content profile

Options	HTTP	FTP	IMAP	POP3	SMTP
Antivirus Scan	☑	☑	☑	☑	☑
File Block	☐	☐	☐	☐	☐
Web URL Block	☐				
Web Content Block	☐				
Web Script Filter	☐				
Web Exempt List	☐				
Email Block List			☐	☐	
Email Exempt List			☐	☐	
Email Content Block			☐	☐	
Oversized File/Email Block	pass	pass	pass	pass	pass
Pass Fragmented Emails			☐	☐	☐

Web content profile

Use the web content profile to apply antivirus scanning and web content blocking to HTTP content traffic. You can add this content profile to firewall policies that control HTTP traffic.

Table 8: Web content profile

Options	HTTP	FTP	IMAP	POP3	SMTP
Antivirus Scan	☑	☐	☐	☐	☐
File Block	☐	☐	☐	☐	☐
Web URL Block	☑				
Web Content Block	☑				
Web Script Filter	☐				
Web Exempt List	☐				
Email Block List	☐		☐	☐	
Email Exempt List			☐	☐	
Email Content Block			☐	☐	
Oversized File/Email Block	pass	pass	pass	pass	pass
Pass Fragmented Emails			☐	☐	☐

Unfiltered content profile

Use the unfiltered content profile if you do not want to apply content protection to traffic. You can add this content profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected.

Table 9: Unfiltered content profile

Options	HTTP	FTP	IMAP	POP3	SMTP
Antivirus Scan	☐	☐	☐	☐	☐
File Block	☐	☐	☐	☐	☐
Web URL Block	☐				
Web Content Block	☐				
Web Script Filter	☐				
Web Exempt List	☑				
Email Block List	☐		☐	☐	
Email Exempt List			☑	☑	
Email Content Block			☐	☐	
Oversized File/Email Block	pass	pass	pass	pass	pass
Pass Fragmented Emails			☑	☑	☑

Planning the FortiGate configuration

Before you configure the FortiGate unit, you need to plan how to integrate the unit into the network. Among other things, you must decide whether you want the unit to be visible to the network, which firewall functions you want it to provide, and how you want it to control the traffic flowing between its interfaces.

Your configuration plan depends on the operating mode that you select. The FortiGate unit can be configured in one of two modes: NAT/Route mode (the default) or Transparent mode.

NAT/Route mode

In NAT/Route mode, the unit is visible to the network. Like a router, all its interfaces are on different subnets. The following interfaces are available in NAT/Route mode:

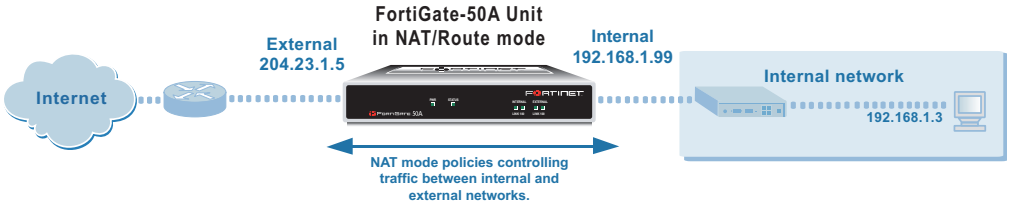
- External is the interface to the external network (usually the Internet).
- Internal is the interface to the internal network.

You can add security policies to control whether communications through the FortiGate unit operate in NAT or Route mode. Security policies control the flow of traffic based on the source address, destination address, and service of each packet. In NAT mode, the FortiGate unit performs network address translation before it sends the packet to the destination network. In Route mode, there is no translation.

By default, the FortiGate unit has a NAT mode security policy that allows users on the internal network to securely download content from the external network. No other traffic is possible until you have configured further security policies.

You typically use NAT/Route mode when the FortiGate unit is operating as a gateway between private and public networks. In this configuration, you would create NAT mode policies to control traffic flowing between the internal, private network and the external, public network (usually the Internet).

Figure 3: Example NAT/Route mode network configuration

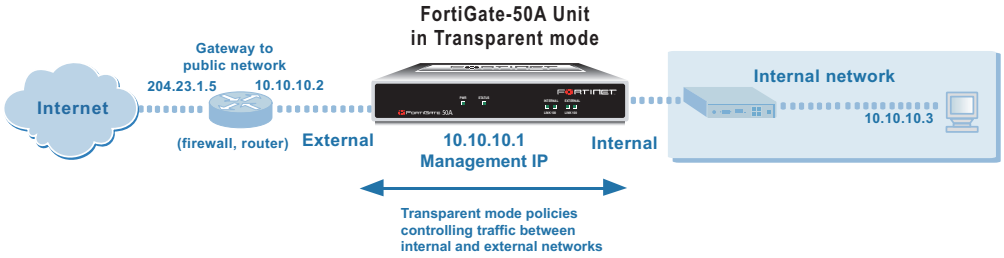


Transparent mode

In Transparent mode, the FortiGate unit is invisible to the network. Similar to a network bridge, all FortiGate interfaces must be on the same subnet. You only have to configure a management IP address so that you can make configuration changes. The management IP address is also used for antivirus and attack definition updates.

You typically use the FortiGate unit in Transparent mode on a private network behind an existing firewall or behind a router. The FortiGate unit performs firewall functions as well as antivirus and content scanning but not VPN.

Figure 4: Example Transparent mode network configuration



Configuration options

Once you have selected Transparent or NAT/Route mode operation, you can complete the configuration plan and begin to configure the FortiGate unit.

You can use the web-based manager setup wizard or the command line interface (CLI) for the basic configuration of the FortiGate unit.

Setup wizard

If you are configuring the FortiGate unit to operate in NAT/Route mode (the default), the setup wizard prompts you to add the administration password and internal interface address. The setup wizard also prompts you to choose either a manual (static) or a dynamic (DHCP or PPPoE) address for the external interface. Using the wizard, you can also add DNS server IP addresses and a default route for the external interface.

In NAT/Route mode you can also change the configuration of the FortiGate DHCP server to supply IP addresses for the computers on your internal network. You can also configure the FortiGate to allow Internet access to your internal Web, FTP, or email servers.

If you are configuring the FortiGate unit to operate in Transparent mode, you can switch to Transparent mode from the web-based manager and then use the setup wizard to add the administration password, the management IP address and gateway, and the DNS server addresses.

CLI

If you are configuring the FortiGate unit to operate in NAT/Route mode, you can add the administration password and the Internal interface address. You can also use the CLI to configure the external interface for either a manual (static) or a dynamic (DHCP or PPPoE) address. Using the CLI, you can also add DNS server IP addresses and a default route for the external interface.

In NAT/Route mode you can also change the configuration of the FortiGate DHCP server to supply IP addresses for the computers on your internal network.

If you are configuring the FortiGate unit to operate in Transparent mode, you can use the CLI to switch to Transparent mode, Then you can add the administration password, the management IP address and gateway, and the DNS server addresses.

FortiGate model maximum values matrix

Table 10: FortiGate maximum values matrix

	FortiGate model											
	50A	**60**	**100**	**200**	**300**	**400**	**500**	**800**	**1000**	**3000**	**3600**	**4000**
Routes	500	500	500	500	500	500	500	500	500	500	500	500
Policy routing gateways	500	500	500	500	500	500	500	500	500	500	500	500
Administrative users	500	500	500	500	500	500	500	500	500	500	500	500
VLAN subinterfaces	N/A	N/A	N/A	4096*	4096*	4096*	4096*	4096*	4096*	4096*	4096*	4096*
Zones	N/A	N/A	N/A	100	100	100	100	100	200	300	500	500
Virtual domains	N/A	N/A	N/A	16	32	64	64	64	128	512	512	512
DHCP address scopes	32	32	32	32	32	32	32	32	32	32	32	32
DHCP reserved IP/MAC pairs	10	20	30	30	50	50	100	100	200	200	200	200
Firewall policies	200	500	1000	2000	5000	5000	20000	20000	50000	50000	50000	50000
Firewall addresses	500	500	500	500	3000	3000	6000	6000	10000	10000	10000	10000
Firewall address groups	500	500	500	500	500	500	500	500	500	500	500	500
Firewall custom services	500	500	500	500	500	500	500	500	500	500	500	500
Firewall service groups	500	500	500	500	500	500	500	500	500	500	500	500
Firewall recurring schedules	256	256	256	256	256	256	256	256	256	256	256	256
Firewall onetime schedules	256	256	256	256	256	256	256	256	256	256	256	256
Firewall virtual IPs	500	500	500	500	500	500	500	500	500	500	500	500
Firewall IP pools	50	50	50	50	50	50	50	50	50	50	50	50
IP/MAC binding table entries	500	500	500	500	500	500	500	500	500	500	500	500
Firewall content profiles	32	32	32	32	32	32	32	32	32	32	32	32
User names	20	500	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
Radius servers	6	6	6	6	6	6	6	6	6	6	6	6
LDAP servers	6	6	6	6	6	6	6	6	6	6	6	6
User groups	100	100	100	100	100	100	100	100	100	100	100	100
Total number of user group members	300	300	300	300	300	300	300	300	300	300	300	300
* Includes the number of physical interfaces.												

Table 10: FortiGate maximum values matrix

	FortiGate model											
	50A	**60**	**100**	**200**	**300**	**400**	**500**	**800**	**1000**	**3000**	**3600**	**4000**
IPSec remote gateways (Phase 1)	20	50	80	200	1500	1500	3000	3000	5000	5000	5000	5000
IPSec VPN tunnels (Phase 2)	20	50	80	200	1500	1500	3000	3000	5000	5000	5000	5000
IPSec VPN concentrators	500	500	500	500	500	500	500	500	500	500	500	500
PPTP users	500	500	500	500	500	500	500	500	500	500	500	500
L2TP users	500	500	500	500	500	500	500	500	500	500	500	500
NIDS user-defined signatures	100	100	100	100	100	100	100	100	100	100	100	100
Antivirus file block patterns	56	56	56	56	56	56	56	56	56	56	56	56
Web filter and email filter lists	Limit varies depending on available system memory. Fortinet recommends limiting total size of web and email filter lists to 4 Mbytes or less. If you want to use larger web filter lists, consider using Cerberian web filtering.											
Log setting traffic filter entries	50	50	50	50	50	50	50	50	50	50	50	50
* Includes the number of physical interfaces.												

Next steps

Now that your FortiGate unit is operating, you can proceed to configure it to connect to networks:

- If you are going to operate the FortiGate unit in NAT/Route mode, go to "NAT/Route mode installation" on page 33.
- If you are going to operate the FortiGate unit in Transparent mode, go to "Transparent mode installation" on page 41.

NAT/Route mode installation

This chapter describes how to install the FortiGate unit in NAT/Route mode. To install the FortiGate unit in Transparent mode, see "Transparent mode installation" on page 41.

This chapter describes:

Installing the FortiGate unit using the default configuration

Depending on your requirements, you may be able to deploy the FortiGate unit without changing its factory default configuration. If the factory default settings in Table 11 are compatible with your requirements, all you need to do is configure your internal network and then connect the FortiGate unit.

Table 11: FortiGate unit factory default configuration

Operating Mode	NAT/Route mode.
Firewall Policy	One NAT mode policy that allows users on the internal network to access any Internet service. No other traffic is allowed. All web and email traffic is scanned for viruses.
External interface	The External interface receives its IP address by DHCP from your Internet Service Provider (ISP).
DHCP Server on internal network	The FortiGate unit functions as a DHCP server for your internal network. If you configure the computers on your internal network to obtain an IP address automatically using DHCP, the FortiGate unit automatically sets the IP addresses of the computers in this range: Starting IP: 192.168.1.1 Ending IP: 192.168.1.254 One IP address is reserved for the FortiGate internal interface: 192.168.1.99.

To use the factory default configuration, follow these steps to install the FortiGate unit:

1. Configure the TCP/IP settings of the computers on your internal network to obtain an IP address automatically using DHCP. Refer to your computer documentation for assistance.
2. Complete the procedure in the section "Connecting the FortiGate unit to your networks" on page 37.

Changing the default configuration

You can use the procedures in this chapter to change the default configuration. For example, if your ISP assigns IP addresses using PPPoE instead of DHCP, you only need to change the configuration of the external interface. Use the information in the rest of this chapter to change the default configuration as required.

Preparing to configure NAT/Route mode

Use Table 12 to gather the information that you need to customize NAT/Route mode settings.

Table 12: NAT/Route mode settings

Administrator password:		
Internal interface	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
External interface	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
	Default Gateway:	_____ . _____ . _____ . _____
	Primary DNS Server:	_____ . _____ . _____ . _____
	Secondary DNS Server:	_____ . _____ . _____ . _____
Internal servers	Web Server:	_____ . _____ . _____ . _____
	SMTP Server:	_____ . _____ . _____ . _____
	POP3 Server:	_____ . _____ . _____ . _____
	IMAP Server:	_____ . _____ . _____ . _____
	FTP Server:	_____ . _____ . _____ . _____
	If you provide access from the Internet to a web server, mail server, IMAP server, or FTP server installed on an internal network, add the IP addresses of the servers here.	

Advanced NAT/Route mode settings

Use Table 13 to gather the information that you need to customize advanced FortiGate NAT/Route mode settings.

Table 13: Advanced FortiGate NAT/Route mode settings

DHCP server	Starting IP:	_____ . _____ . _____ . _____
	Ending IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
	Default Route:	_____ . _____ . _____ . _____
	DNS IP:	_____ . _____ . _____ . _____
	The FortiGate unit contains a DHCP server that you can configure to automatically set the addresses of the computers on your internal network.	

Using the setup wizard

From the web-based manager, you can use the setup wizard to create the initial configuration of your FortiGate unit. To connect to the web-based manager, see "Connecting to the web-based manager" on page 19.

Starting the setup wizard

1. Select Easy Setup Wizard (the middle button in the upper-right corner of the web-based manager).
2. Use the information that you gathered in Table 12 on page 34 to fill in the wizard fields. Select the Next button to step through the wizard pages.
3. Confirm your configuration settings and then select Finish and Close.

Note: If you use the setup wizard to configure internal server settings, the FortiGate unit adds port forwarding virtual IPs and firewall policies for each server. For each server located on your internal network the FortiGate unit adds an Ext->Int policy.

Reconnecting to the web-based manager

If you used the setup wizard to change the IP address of the internal interface, you must reconnect to the web-based manager using a new IP address. Browse to https:// followed by the new IP address of the internal interface. Otherwise, you can reconnect to the web-based manager by browsing to https://192.168.1.99.

You have now completed the initial configuration of your FortiGate unit, and you can proceed to "Connecting the FortiGate unit to your networks" on page 37.

Using the command line interface

As an alternative to using the setup wizard, you can configure the FortiGate unit using the command line interface (CLI). To connect to the CLI, see "Connecting to the command line interface (CLI)" on page 20.

Configuring the FortiGate unit to operate in NAT/Route mode

Use the information that you gathered in Table 12 on page 34 to complete the following procedures.

Configuring NAT/Route mode IP addresses

1. Log into the CLI if you are not already logged in.
2. Set the IP address and netmask of the internal interface to the internal IP address and netmask that you recorded in Table 12 on page 34. Enter:

   ```
   set system interface internal mode static ip <IP address>
   <netmask>
   ```

   Example

   ```
   set system interface internal mode static ip 192.168.1.1
   255.255.255.0
   ```

3. Set the IP address and netmask of the external interface to the external IP address and netmask that you recorded in Table 12 on page 34.

   To set the manual IP address and netmask, enter:

   ```
   set system interface external static ip <IP address> <netmask>
   ```

   Example

   ```
   set system interface external mode static ip 204.23.1.5
   255.255.255.0
   ```

   To set the external interface to use DHCP, enter:

   ```
   set system interface external mode dhcp connection enable
   ```

   To set the external interface to use PPPoE, enter:

   ```
   set system interface external mode pppoe username <user name>
   password <password> connection enable
   ```

   Example

   ```
   set system interface external mode pppoe username
   user@domain.com password mypass connection enable
   ```

4. Confirm that the addresses are correct. Enter:

   ```
   get system interface
   ```

   The CLI lists the IP address, netmask and other settings for each of the FortiGate interfaces.

5. Set the primary DNS server IP addresses. Enter

   ```
   set system dns primary <IP address>
   ```

   Example

   ```
   set system dns primary 293.44.75.21
   ```

6 Optionally, set the secondary DNS server IP addresses. Enter

```
set system dns secondary <IP address>
```

Example

```
set system dns secondary 293.44.75.22
```

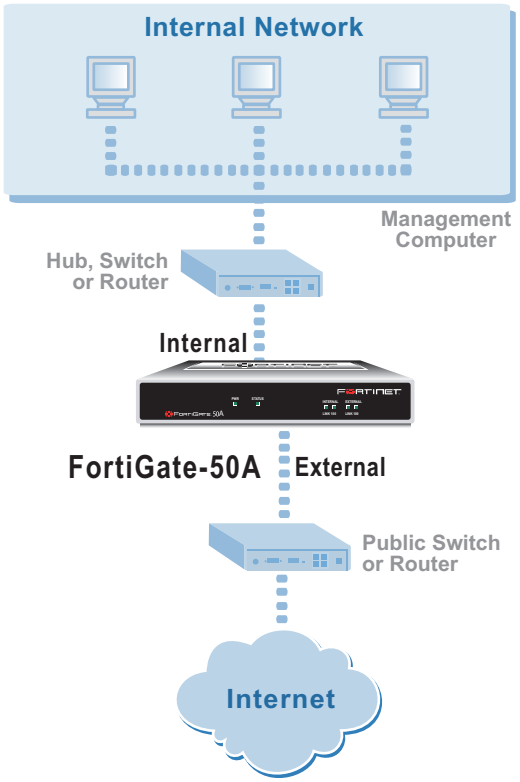
7 Set the default route to the Default Gateway IP address (not required for DHCP and PPPoE).

```
set system route number <route_no> dst 0.0.0.0 0.0.0.0 gw1
<gateway_ip>
```

Example

```
set system route number 0 dst 0.0.0.0 0.0.0.0 gw1 204.23.1.2
```

Figure 5: FortiGate-50A network connections



Connecting the FortiGate unit to your networks

When you have completed the initial configuration, you can connect the FortiGate unit between your internal network and the Internet.

There are two 10/100 BaseTX connectors on the FortiGate-50A:

- Internal for connecting to your internal network,
- External for connecting to the Internet.

To connect the FortiGate-50A unit:

1 Connect the Internal interface to the hub or switch connected to your internal network.

2 Connect the External interface to the Internet.

Connect to the public switch or router provided by your Internet Service Provider. If you are a DSL or cable subscriber, connect the External interface to the internal or LAN connection of your DSL or cable modem.

Configuring your networks

If you are operating the FortiGate unit in NAT/Route mode, your internal network must be configured to route all Internet traffic to the FortiGate internal interface. Change the default gateway address of all computers and routers connected directly to your internal network to the IP address of the FortiGate internal interface. For the external network, route all packets to the FortiGate external interface.

If you are using the FortiGate unit as the DHCP server for your internal network, configure the computers on your internal network for DHCP.

Make sure that the connected FortiGate unit is functioning properly by connecting to the Internet from a computer on your internal network. You should be able to connect to any Internet address.

Completing the configuration

Use the information in this section to complete the initial configuration of the FortiGate unit.

Setting the date and time

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

To set the FortiGate system date and time, see “Setting system date and time” on page 121.

Changing antivirus protection

By default, the FortiGate unit scans all web and email content for viruses. You can use the following procedure to change the antivirus configuration. To change the antivirus configuration:

1 Select Edit  to edit this policy.

2 For Anti-Virus & Web Filter you can select a different Content Profile.

See “Factory default content profiles” on page 25 for descriptions of the default content profiles.

3 Select OK to save your changes.

You can also add you own content profiles. See “Adding content profiles” on page 167.

Registering your FortiGate unit

After purchasing and installing a new FortiGate unit, you can register the unit by going to System > Update > Support, or 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 you or your organization have purchased. Registration is quick and easy. You can register multiple FortiGate units in a single session without re-entering your contact information.

For more information about registration, see “Registering FortiGate units” on page 83.

Configuring virus and attack definition updates

You can go to System > Update to configure the FortiGate unit to automatically check to see if new versions of the virus definitions and attack definitions are available. If it finds new versions, the FortiGate unit automatically downloads and installs the updated definitions.

The FortiGate unit uses HTTPS on port 8890 to check for updates. The FortiGate external interface must have a path to the FortiResponse Distribution Network (FDN) using port 8890.

To configure automatic virus and attack updates, see “Updating antivirus and attack definitions” on page 73.

Transparent mode installation

This chapter describes how to install your FortiGate unit in Transparent mode. If you want to install the FortiGate unit in NAT/Route mode, see "NAT/Route mode installation" on page 33.

This chapter describes:

Preparing to configure Transparent mode

Use Table 14 to gather the information that you need to customize Transparent mode settings.

Table 14: Transparent mode settings

Administrator Password:		
Management IP	IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
	Default Gateway:	_____ . _____ . _____ . _____
	The management IP address and netmask must be valid for the network from which you will manage the FortiGate unit. Add a default gateway if the FortiGate unit must connect to a router to reach the management computer.	
DNS Settings	Primary DNS Server:	_____ . _____ . _____ . _____
	Secondary DNS Server:	_____ . _____ . _____ . _____

Using the setup wizard

From the web-based manager, you can use the setup wizard to create the initial configuration of your FortiGate unit. To connect to the web-based manager, see “Connecting to the web-based manager” on page 19.

Changing to Transparent mode

The first time that you connect to the FortiGate unit, it is configured to run in NAT/Route mode. To switch to Transparent mode using the web-based manager:

1. Go to **System > Status**.
2. Select Change to Transparent Mode.
3. Select Transparent in the Operation Mode list.
4. Select OK.

   The FortiGate unit changes to Transparent mode.

   To reconnect to the web-based manager, change the IP address of your management computer to 10.10.10.2. Connect to the internal or DMZ interface and browse to https:// followed by the Transparent mode management IP address. The default FortiGate Transparent mode management IP address is 10.10.10.1.

Starting the setup wizard

1. Select Easy Setup Wizard (the middle button in upper-right corner of the web-based manager).
2. Use the information that you gathered in Table 14 on page 41 to fill in the wizard fields. Select the Next button to step through the wizard pages.
3. Confirm your configuration settings and then select Finish and Close.

Reconnecting to the web-based manager

If you changed the IP address of the management interface while you were using the setup wizard, you must reconnect to the web-based manager using the new IP address. Browse to https:// followed by the new IP address of the management interface. Otherwise, you can reconnect to the web-based manager by browsing to https://10.10.10.1. If you connect to the management interface through a router, make sure that you have added a default gateway for that router to the management IP default gateway field.

Using the command line interface

As an alternative to the setup wizard, you can configure the FortiGate unit using the command line interface (CLI). To connect to the CLI, see “Connecting to the command line interface (CLI)” on page 20. Use the information that you gathered in Table 14 on page 41 to complete the following procedures.

Changing to Transparent mode

1. Log into the CLI if you are not already logged in.
2. Switch to Transparent mode. Enter:
   ```
   set system opmode transparent
   ```
   After a few seconds, the login prompt appears.
3. Type `admin` and press Enter.
   The following prompt appears:
   ```
   Type ? for a list of commands.
   ```
4. Confirm that the FortiGate unit has switched to Transparent mode. Enter:
   ```
   get system status
   ```
   The CLI displays the status of the FortiGate unit. The last line shows the current operation mode.
   ```
   Operation mode: Transparent
   ```

Configuring the Transparent mode management IP address

1. Log into the CLI if you are not already logged in.
2. Set the management IP address and netmask to the IP address and netmask that you recorded in Table 14 on page 41. Enter:
   ```
   set system management ip <IP address> <netmask>
   ```
   Example
   ```
   set system management ip 10.10.10.2 255.255.255.0
   ```
3. Confirm that the address is correct. Enter:
   ```
   get system management
   ```
   The CLI lists the management IP address and netmask.

Configure the Transparent mode default gateway

1. Log into the CLI if you are not already logged in.
2. Set the default route to the default gateway that you recorded in Table 14 on page 41. Enter:
   ```
   set system route number <number> gateway <IP address>
   ```
   Example
   ```
   set system route number 1 gw1 204.23.1.2
   ```
   You have now completed the initial configuration of the FortiGate unit.

Connecting the FortiGate unit to your networks

When you have completed the initial configuration, you can connect the FortiGate unit between your internal network and the Internet.

There are two 10/100 BaseTX connectors on the FortiGate-50A unit:

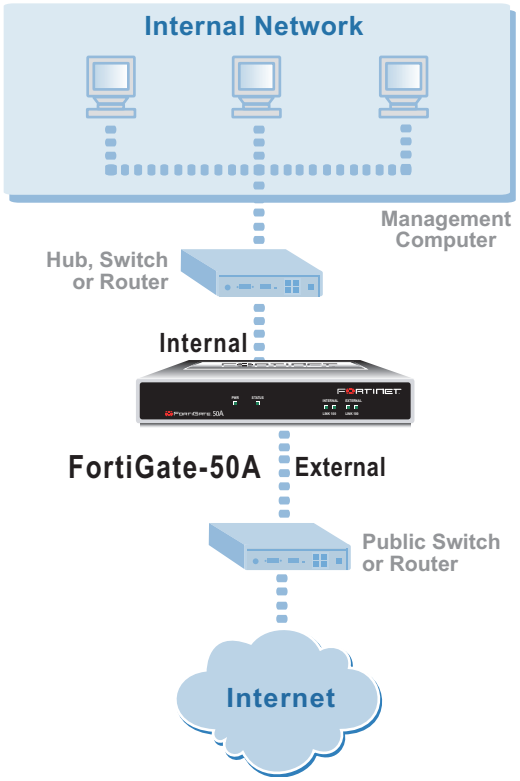
- Internal for connecting to your internal network,
- External for connecting to the Internet.

To connect the FortiGate unit:

1 Connect the Internal interface to the hub or switch connected to your internal network.

2 Connect the External interface to the Internet.
Connect to the public switch or router provided by your Internet Service Provider.

Figure 6: FortiGate-50A network connections



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 would be deployed in Transparent mode when it is intended to provide antivirus and content scanning behind an existing firewall solution.

A FortiGate unit in Transparent mode can also perform firewalling. Even though it takes no part in the layer 3 topology, it can examine layer 3 header information and make decisions on whether to block or pass traffic.

Completing the configuration

Use the information in this section to complete the initial configuration of the FortiGate unit.

Setting the date and time

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

To set the FortiGate system date and time, see “Setting system date and time” on page 121.

Enabling antivirus protection

To enable antivirus protection to protect users on your internal network from downloading a virus from the Internet:

1. Go to **Firewall > Policy > Int–>Ext**.
2. Select Edit  to edit this policy.
3. Select Anti-Virus & Web filter to enable antivirus protection for this policy.
4. Select the Scan Content Profile.
5. Select OK to save your changes.

Registering your FortiGate

After purchasing and installing a new FortiGate unit, you can register the unit by going to System > Update > Support, or 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 you or your organization have purchased. Registration is quick and easy. You can register multiple FortiGate units in a single session without re-entering your contact information.

For more information about registration, see “Registering FortiGate units” on page 83.

Configuring virus and attack definition updates

You can configure the FortiGate unit to automatically check to see if new versions of the virus definitions and attack definitions are available. If it finds new versions, the FortiGate unit automatically downloads and installs the updated definitions.

The FortiGate unit uses HTTPS on port 8890 to check for updates. The FortiGate external interface must have a path to the FortiResponse Distribution Network (FDN) using port 8890.

To configure automatic virus and attack updates, see “Updating antivirus and attack definitions” on page 73.

Transparent mode configuration examples

A FortiGate unit operating in Transparent mode still requires a basic configuration to operate as a node on the IP network. As a minimum, the FortiGate unit must be configured with an IP address and subnet mask. These are used for management access and to allow the unit to receive antivirus and definitions updates. Also, the unit must have sufficient route information to reach:

- the management computer,
- The FortiResponse Distribution Network (FDN),
- a DNS server.

A route is required whenever the FortiGate unit connects to a router to reach a destination. If all of the destinations are located on the external network, you may be required to enter only a single default route. If, however, the network topology is more complex, you may be required to enter one or more static routes in addition to the default route.

This section describes:

Default routes and static routes

To create a route to a destination, you need to define an IP prefix which consists of an IP network address and a corresponding netmask value. A default route matches any prefix and forwards traffic to the next hop router (otherwise known as the default gateway). A static route matches a more specific prefix and forwards traffic to the next hop router.

Default route example:

IP Prefix 0.0.0.0 (IP address)
0.0.0.0 (Netmask)
Next Hop 192.168.1.2

Static Route example:

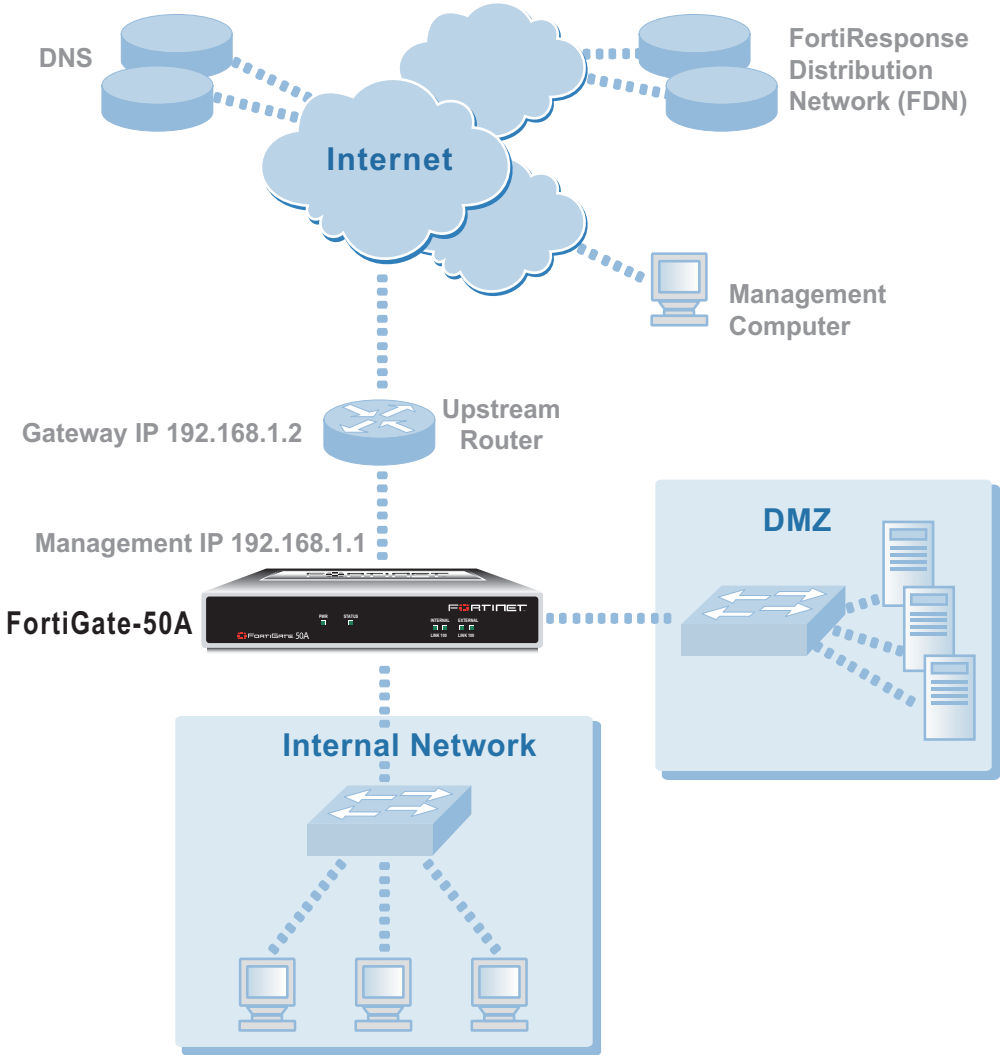
IP Prefix 172.100.100.0 (IP address)
255.255.255.0 (Netmask)
Next Hop 192.168.1.2

Note: When adding routes to the FortiGate unit, add the default route last so that it appears on the bottom of the route list. This ensures that the unit will attempt to match more specific routes before selecting the default route.

Example default route to an external network

Figure 7 shows a FortiGate unit where all destinations, including the management computer, are located on the external network. To reach these destinations, the FortiGate unit must connect to the “upstream” router leading to the external network. To facilitate this connection, you must enter a single default route that points to the upstream router as the next hop/default gateway.

Figure 7: Default route to an external network



General configuration steps

1. Set the FortiGate unit to operate in Transparent mode.
2. Configure the Management IP address and Netmask of the FortiGate unit.
3. Configure the default route to the external network.

Web-based manager example configuration steps

To configure basic Transparent mode settings and a default route using the web-based manager:

1 Go to **System > Status**.
- Select Change to Transparent Mode.
- Select Transparent in the Operation Mode list.
- Select OK.

  The FortiGate unit changes to Transparent mode.

2 Go to **System > Network > Management**.
- Change the Management IP and Netmask:

  IP: 192.168.1.1

  Mask: 255.255.255.0
- Select Apply.

3 Go to **System > Network > Routing**.
- Select New to add the default route to the external network.

  Destination IP: 0.0.0.0

  Mask: 0.0.0.0

  Gateway: 192.168.1.2
- Select OK.

CLI configuration steps

To configure the Fortinet basic settings and a default route using the CLI:

1 Change the system to operate in Transparent Mode.

```
set system opmode transparent
```

2 Add the Management IP address and Netmask.

```
set system management ip 192.168.1.1 255.255.255.0
```

3 Add the default route to the external network.

```
set system route number 1 gw1 192.168.1.2
```

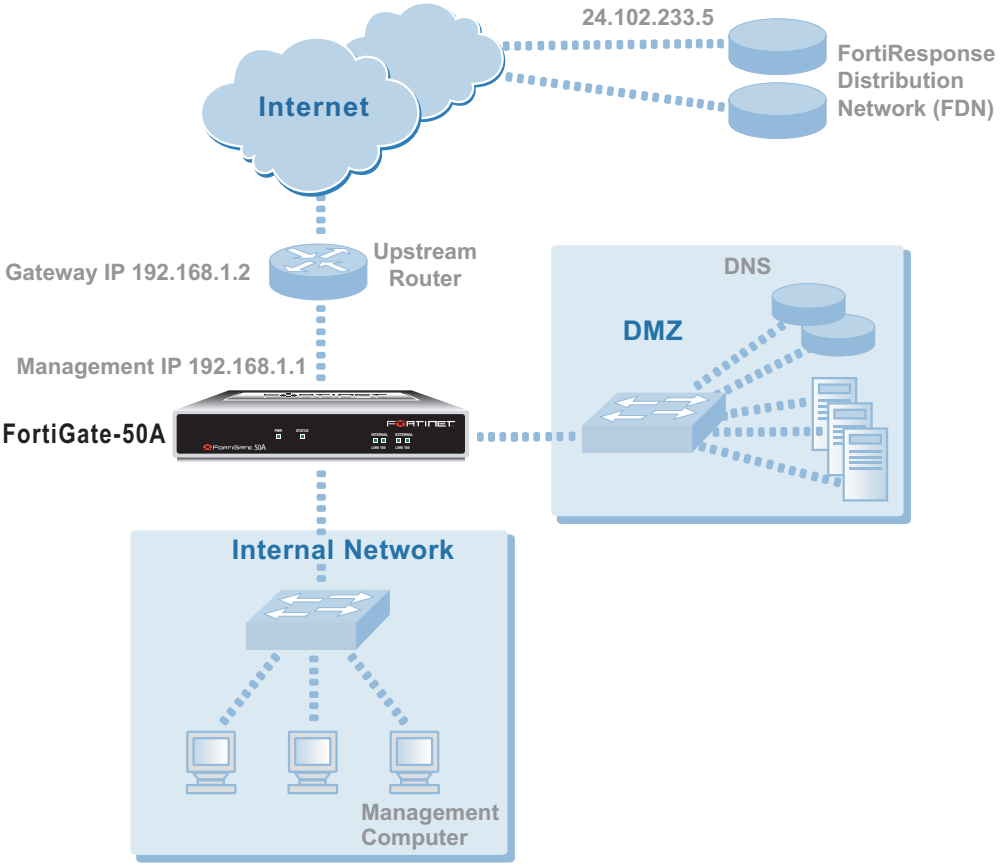
Example static route to an external destination

Figure 8 shows a FortiGate unit that requires routes to the FDN located on the external network. The Fortigate unit does not require routes to the DNS servers or management computer because they are located on the internal network.

To connect to the FDN, you would typically enter a single default route to the external network. However, to provide an extra degree of security, you could enter static routes to a specific FortiResponse server in addition to a default route to the external network. If the static route becomes unavailable (perhaps because the IP address of the FortiResponse server changes) the FortiGate unit will still be able to receive antivirus and NIDS updates from the FDN using the default route.

Note: This is an example configuration only. To configure a static route, you require a destination IP address.

Figure 8: Static route to an external destination



General configuration steps

1. Set the FortiGate unit to operate in Transparent mode.
2. Configure the Management IP address and Netmask of the FortiGate unit.
3. Configure the static route to the FortiResponse server.
4. Configure the default route to the external network.

Web-based manager example configuration steps

To configure the basic FortiGate settings and a static route using the web-based manager:

1 Go to **System > Status**.
- Select Change to Transparent Mode.
- Select Transparent in the Operation Mode list.
- Select OK.

  The FortiGate unit changes to Transparent mode.

2 Go to **System > Network > Management**.
- Change the Management IP and Netmask:

  IP: 192.168.1.1

  Mask: 255.255.255.0
- Select Apply.

3 Go to **System > Network > Routing**.
- Select New to add the static route to the FortiResponse server.

  Destination IP: 24.102.233.5

  Mask: 255.255.255.0

  Gateway: 192.168.1.2
- Select OK.
- Select New to add the default route to the external network.

  Destination IP: 0.0.0.0

  Mask: 0.0.0.0

  Gateway: 192.168.1.2
- Select OK.

CLI configuration steps

To configure the Fortinet basic settings and a static route using the CLI:

1 Set the system to operate in Transparent Mode.

```
set system opmode transparent
```

2 Add the Management IP address and Netmask.

```
set system management ip 192.168.1.1 255.255.255.0
```

3 Add the static route to the primary FortiResponse server.

```
set system route number 1 dst 24.102.233.5 255.255.255.0 gw1
  192.168.1.2
```

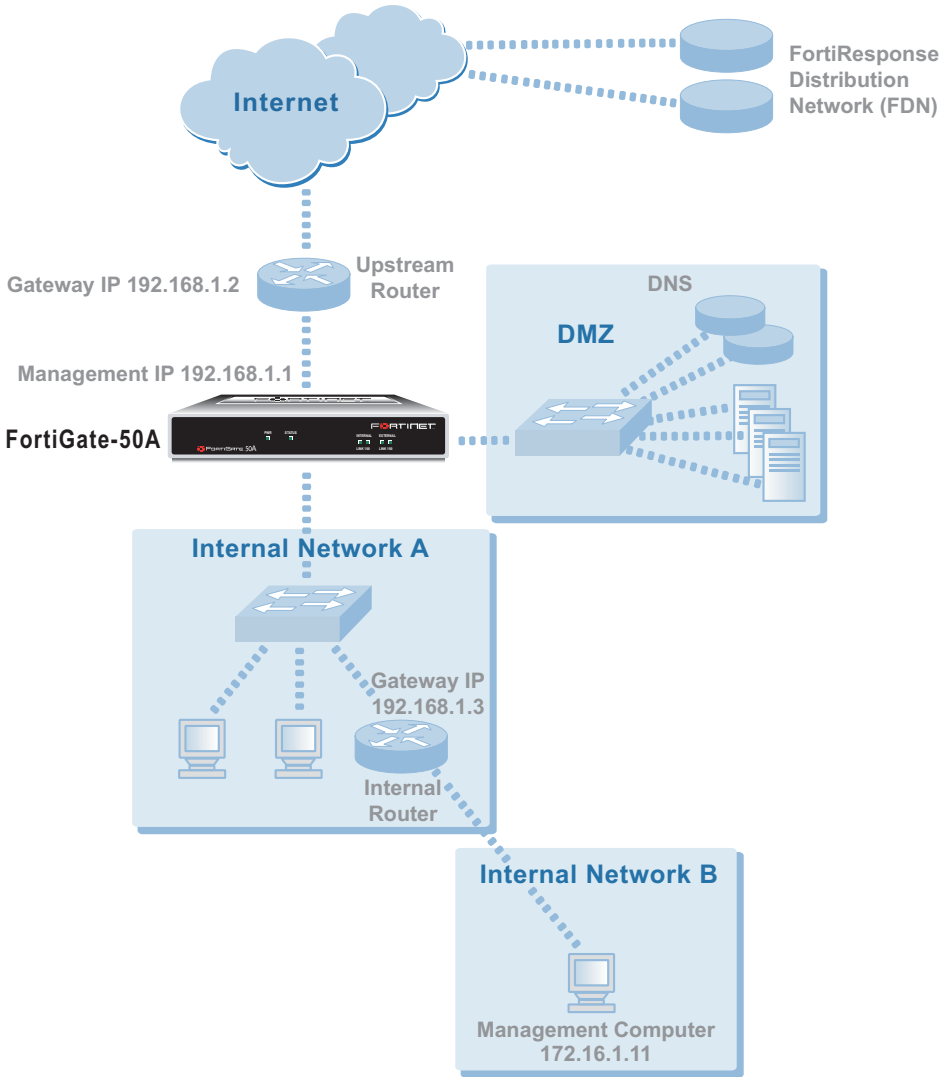
4 Add the default route to the external network.

```
set system route number 2 gw1 192.168.1.2
```

Example static route to an internal destination

Figure 9 shows a FortiGate unit where the FDN is located on an external subnet and the management computer is located on a remote, internal subnet. To reach the FDN, you need to enter a single default route that points to the upstream router as the next hop/default gateway. To reach the management computer, you need to enter a single static route that leads directly to it. This route will point to the internal router as the next hop. (No route is required for the DNS servers because they are on the same layer 3 subnet as the FortiGate unit.)

Figure 9: Static route to an internal destination



General configuration steps

1. Set the unit to operate in Transparent mode.
2. Configure the Management IP address and Netmask of the FortiGate unit.
3. Configure the static route to the management computer on the internal network.

4 Configure the default route to the external network.

Web-based manager example configuration steps

To configure the FortiGate basic settings, a static route, and a default route using the web-based manager:

1 Go to **System > Status**.
- Select Change to Transparent Mode.
- Select Transparent in the Operation Mode list.
- Select OK.

  The FortiGate unit changes to Transparent mode.

2 Go to **System > Network > Management**.
- Change the Management IP and Netmask:

  IP: 192.168.1.1

  Mask: 255.255.255.0
- Select Apply.

3 Go to **System > Network > Routing**.
- Select New to add the static route to the management computer.

  Destination IP: 172.16.1.11

  Mask: 255.255.255.0

  Gateway: 192.168.1.3
- Select OK.
- Select New to add the default route to the external network.

  Destination IP: 0.0.0.0

  Mask: 0.0.0.0

  Gateway: 192.168.1.2
- Select OK.

CLI configuration steps

To configure the FortiGate basic settings, a static route, and a default route using the CLI:

1 Set the system to operate in Transparent Mode.

```
set system opmode transparent
```

2 Add the Management IP address and Netmask.

```
set system management ip 192.168.1.1 255.255.255.0
```

3 Add the static route to the management computer.

```
set system route number 1 dst 172.16.1.11 255.255.255.0 gw1
  192.168.1.3
```

4 Add the default route to the external network.

```
set system route number 2 gw1 192.168.1.2
```

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 current firmware version, the current virus and attack definitions, and the FortiGate unit serial number.

If you log into the web-based manager using the admin administrator account, you can make any of the following changes to the FortiGate system settings:

- Changing the FortiGate host name
- Changing the FortiGate firmware
- Manual virus definition updates
- Manual attack definition updates
- Backing up system settings
- Restoring system settings
- Restoring system settings to factory defaults
- Changing to Transparent mode
- Changing to NAT/Route mode
- Restarting the FortiGate unit
- Shutting down the FortiGate unit

If you log into the web-based manager with another administrator account, you can view the system settings including:

- Displaying the FortiGate serial number
- Displaying the FortiGate up time

All administrative users can also go to the Monitor page and view FortiGate system status. System status displays FortiGate system health monitoring information, including CPU and memory status, session and network status.

- System status

All administrative users can also go to the Session page and view the active communication sessions to and through the FortiGate unit.

- Session list

Changing the 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 “Configuring SNMP” on page 125.

The default host name is FortiGate-50A.

To change the FortiGate host name

1 Go to **System > Status**.

2 Select Edit Host Name  .

3 Type a new host name.

4 Select OK.

The new host name is displayed on the Status page, and in the CLI prompt, and is added to the SNMP System Name.

Changing 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
Upgrading to a new firmware version	Commonly-used web-based manager and CLI procedures to upgrade to a new FortiOS firmware version or to a more recent build of the same firmware version.
Reverting to a previous firmware version	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.
Installing firmware images from a system reboot using the CLI	Use this procedure to install a new firmware version or revert to a previous firmware version. You must run this procedure by connecting to the CLI using the FortiGate console port and a null-modem cable. This procedure reverts the FortiGate unit to its factory default configuration.
Testing a new firmware image before installing it	Use this procedure to test a new firmware image before installing it. You must run this procedure by connecting 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.

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 "Manually initiating antivirus and attack definitions updates" on page 75 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.
3. Go to **System > Status**.
4. Select Firmware Upgrade  .
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 antivirus and attack definitions, see "Manually initiating antivirus and attack definitions updates" on page 75.

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 "Manually initiating antivirus and attack definitions updates" on page 75 to make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute updatecenter updatenow` 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 as the admin administrative user.

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_ip>
```

Where `<name_str>` is the name of the firmware image file on the TFTP server and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `FGT_300-v250-build045-FORTINET.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image FGT_300-v250-build045-FORTINET.out
192.168.1.168
```

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

6 Reconnect to the CLI.

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

```
get system status
```

8 Use the procedure "Manually initiating antivirus and attack definitions updates" on page 75 to update antivirus and attack definitions, or from the CLI, enter:

```
execute updatecenter updatenow
```

9 To confirm that the antivirus and attack definitions are successfully updated, enter the following command to display the antivirus engine, virus and attack definitions version, contract expiry, and last update attempt information.

```
get system objver
```

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 delete NIDS user-defined signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure you can:

- Back up the FortiGate unit configuration. For information, see "Backing up system settings" on page 64.
- Back up the NIDS user-defined signatures. For information, see the *FortiGate NIDS Guide*
- Back up web content and email filtering lists. For information, see the *FortiGate Content Protection Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.50 to FortiOS v2.36) 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 "Manually initiating antivirus and attack definitions updates" on page 75 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 your management computer.
2. Log into the FortiGate web-based manager as the admin administrative user.
3. Go to **System > Status**.
4. Select Firmware Upgrade  .
5. Type the path and filename of the previous 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 "Restoring system settings" on page 64.
10. Update antivirus and attack definitions. For information about antivirus and attack definitions, see "Manually initiating antivirus and attack definitions updates" on page 75.

Reverting to a previous firmware version using the CLI

This procedure reverts your FortiGate unit to its factory default configuration and deletes NIDS user-defined signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure you can:

- Back up the FortiGate unit configuration using the command `execute backup config`.
- Back up the NIDS user defined signatures using the command `execute backup nidsuserdefsig`
- Back up web content and email filtering lists. For information, see the *FortiGate Content Protection Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.50 to FortiOS v2.36) 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 "Manually initiating antivirus and attack definitions updates" on page 75 to make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute updatecenter updatenow` 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 new firmware image file to the root directory of the TFTP server.
3. Log into the FortiGate CLI as the admin administrative user.
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_ip>
   ```
   Where `<name_str>` is the name of the firmware image file on the TFTP server and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `FGT_300-v250-build045-FORTINET.out` and the IP address of the TFTP server is 192.168.1.168, enter:
   ```
   execute restore image FGT_300-v250-build045-FORTINET.out
   192.168.1.168
   ```
   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.
   This operation will downgrade the current firmware version!
   Do you want to continue? (y/n)
   ```
6. Type Y.
7. 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. Restore your previous configuration. Use the following command:
    ```
    execute restore config
    ```
11. Update antivirus and attack definitions. For information, see "Manually initiating antivirus and attack definitions updates" on page 75, or from the CLI, enter:
    ```
    execute updatecenter updatenow
    ```

12 To confirm that the antivirus and attack definitions have been updated, enter the following command to display the antivirus engine, virus and attack definitions version, contract expiry, and last update attempt information.

```
get system objver
```

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.

To perform 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 system settings" on page 64.
- Back up the NIDS user defined signatures. For information, see the *FortiGate NIDS Guide.*
- Back up web content and email filtering lists. For information, see the *FortiGate Content Protection Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v2.50 to FortiOS v2.36) 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 "Manually initiating antivirus and attack definitions updates" on page 75 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
```

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

```
Press any key to enter 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:

```
[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.

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

The following message appears:

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

10 Type the address of the internal interface of the FortiGate unit and press Enter.

Note: The local IP address is used only to download the firmware image. After the firmware is installed, the address of this interface is changed back to the default IP address for this interface.

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:

```
Save as Default firmware/Run image without saving:[D/R]
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 addresses if required. You can do this from the CLI using the command:

```
set system interface
```

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

- To restore the FortiGate unit configuration, see "Restoring system settings" on page 64.
- To restore NIDS user defined signatures, see "Adding user-defined signatures" on page 218.
- To restore web content filtering lists, see "Restoring the Banned Word list" on page 233 and "Uploading a URL block list" on page 236
- To restore email filtering lists, see "Uploading the email banned word list" on page 247 and "Uploading an email block list" on page 249.

If you are reverting to a previous firmware version (for example, reverting from FortiOS v2.50 to FortiOS v2.36) you might not be able to restore your previous configuration from the backup up configuration file.

Update the virus and attack definitions to the most recent version, see "Manually initiating antivirus and attack definitions updates" on page 75.

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 55.

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 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:

```
Press any key to enter 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:

```
[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.

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

The following message appears:

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

10 Type the address of the internal interface of the FortiGate unit and press Enter.

Note: The local IP address is used only to download the firmware image. After the firmware is installed, the address of this interface is changed back to the default IP address for this interface.

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.

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

Manual virus definition updates

The Status page of the FortiGate web-based manager displays the current installed versions of the FortiGate antivirus definitions.

Note: For information about configuring the FortiGate unit for automatic antivirus definitions updates, see "Virus and attack definitions updates and registration" on page 73. You can also manually start an antivirus definitions update by going to **System > Update** and selecting Update Now.

To update the antivirus definitions manually

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**.
3. In the Antivirus Definitions Version section, select Definitions Update  .
4. 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.

Manual attack definition updates

The Status page of the FortiGate web-based manager displays the current installed versions of the FortiGate Attack Definitions used by the Network Intrusion Detection System (NIDS).

Note: For information about configuring the FortiGate unit for automatic attack definitions updates, see "Virus and attack definitions updates and registration" on page 73. You can also manually start an attack definitions update by going to **System > Update** and selecting Update Now.

To update the attack definitions manually

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**.
3. In the Attack Definitions Version section, select Definitions Update  .
4. 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** to confirm that the Attack Definitions Version information has updated.

Displaying the FortiGate serial number

1 Go to **System > Status**.
The serial number is displayed on the System Status page of the web-based manager. The serial number is specific to the FortiGate unit and does not change with firmware upgrades.

Displaying the FortiGate up time

1 Go to **System > Status**.
The FortiGate up time displays the time in days, hours, and minutes since the FortiGate unit was last started.

Backing up system settings

You can back up system settings by downloading them to a text file on the management computer.

To back up system settings

1 Go to **System > Status**.
2 Select System Settings Backup.
3 Select Backup System Settings.
4 Type a name and location for the file.
The system settings file is backed up to the management computer.
5 Select Return to go back to the Status page.

Restoring system settings

You can restore system settings by uploading a previously downloaded system settings text file.

To restore system settings

1 Go to **System > Status**.
2 Select System Settings Restore.
3 Enter the path and filename of the system settings file, or select Browse and locate the file.
4 Select OK to restore the system settings file to the FortiGate unit.
The FortiGate unit restarts, loading the new system settings.
5 Reconnect to the web-based manager and review your configuration to confirm that the uploaded system settings have taken effect.

Restoring system settings to factory defaults

Use the following procedure to restore 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.

To restore system settings to factory defaults

1. Go to **System > Status**.
2. Select Restore Factory Defaults.
3. Select OK to confirm.
   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.
   For information about restoring system settings, see “Restoring system settings” on page 64.

Changing to Transparent mode

Use the following procedure to change the FortiGate unit from NAT/Route mode to Transparent mode. After you change the FortiGate unit to Transparent mode, most of the configuration resets to Transparent mode factory defaults.

The following items are not set to Transparent mode factory defaults:

- The admin administrator account password (see “Adding and editing administrator accounts” on page 123)
- Custom replacement messages (see “Replacement messages” on page 133)

To change to Transparent mode

1. Go to **System > Status**.
2. Select Change to Transparent Mode.
3. Select Transparent in the operation mode list.
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.

Changing to NAT/Route mode

Use the following procedure to change the FortiGate unit from Transparent mode to NAT/Route mode. After you change the FortiGate unit to NAT/Route mode, most of the configuration resets to NAT/Route mode factory defaults.

The following items are not set to NAT/Route mode factory defaults:

- The admin administrator account password (see "Adding and editing administrator accounts" on page 123)
- Custom replacement messages (see "Replacement messages" on page 133)

To change to NAT/Route mode

1. Go to **System > Status**.
2. Select Change to NAT Mode.
3. Select NAT/Route in the operation mode list.
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 Transparent mode management IP address is 192.168.1.99.

Restarting the FortiGate unit

1. Go to **System > Status**.
2. Select Restart.
   The FortiGate unit restarts.

Shutting down the FortiGate unit

You can restart the FortiGate unit after shutdown only by turning the power off and then on.

1. Go to **System > Status**.
2. Select Shutdown.
   The FortiGate unit shuts down and all traffic flow stops.

System status

You can use the system status monitor to display FortiGate system health information. The system health information includes memory usage, the number of active communication sessions, and the amount of network bandwidth currently in use. The web-based manager displays current statistics as well as statistics for the previous minute.

You can also view current virus and intrusion status. The web-based manager displays the current number of viruses and attacks as well as a graph of virus and attack levels over the previous 20 hours.

In each case you can set an automatic refresh interval that updates the display every 5 to 30 seconds. You can also refresh the display manually.

Viewing CPU and memory status

Current CPU and memory status indicates how close the FortiGate unit is to running at full capacity. The web-based manager displays CPU and memory usage for core processes only. CPU and memory use for management processes (for example, for HTTPS connections to the web-based manager) is excluded.

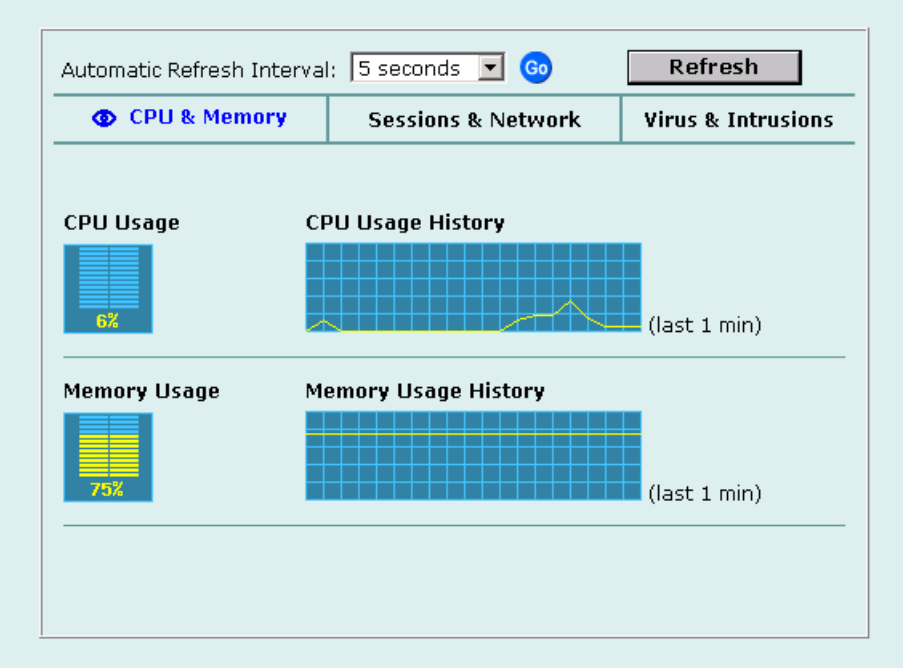
If CPU and memory use is low, the FortiGate unit is able to process much more network traffic than is currently running. If CPU and memory use is high, the FortiGate unit is performing near its full capacity. Putting additional demands on the system might cause traffic processing delays.

CPU and memory intensive processes, such as encrypting and decrypting IPSec VPN traffic, virus scanning, and processing high levels of network traffic containing small packets, increase CPU and memory usage.

To view CPU and memory status

1. Go to **System > Status > Monitor**.
   CPU & Memory status is displayed. The display includes bar graphs of current CPU and memory usage as well as line graphs of CPU and memory usage for the previous minute.
2. Set the automatic refresh interval and select Go to control how often the web-based manager updates the display.
   More frequent updates use system resources and increase network traffic. However, this occurs only when you are viewing the display using the web-based manager.
3. Select Refresh to manually update the information displayed.

Figure 1: CPU and memory status monitor



Viewing sessions and network status

Use the session and network status display to track how many network sessions the FortiGate unit is processing and to see what effect the number of sessions has on the available network bandwidth. Also, by comparing CPU and memory usage with session and network status you can see how much demand network traffic is putting on system resources.

The Sessions section displays the total number of sessions being processed by the FortiGate unit on all interfaces. It also displays the sessions as a percentage of the maximum number of sessions that the FortiGate unit is designed to support.

The Network utilization section displays the total network bandwidth being used through all FortiGate interfaces. It also displays network utilization as a percentage of the maximum network bandwidth that can be processed by the FortiGate unit.

To view sessions and network status

1 Go to **System > Status > Monitor**.

2 Select Sessions & Network.

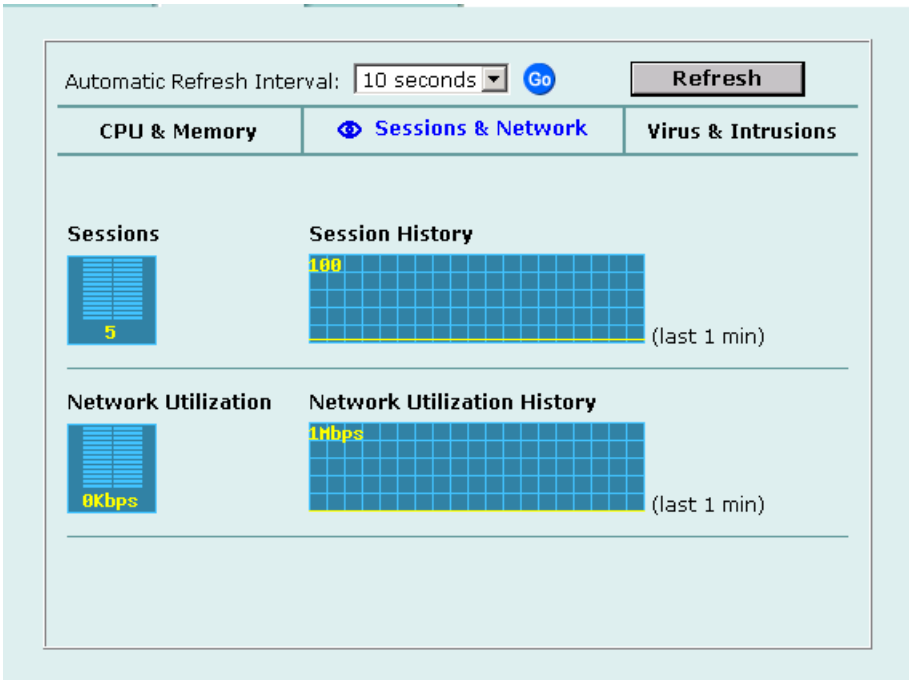
Sessions and network status is displayed. The display includes bar graphs of the current number of sessions and current network utilization as well as line graphs of session and network utilization usage for the last minute. The line graph scales are shown in the upper left corner of the graph.

3 Set the automatic refresh interval and select Go to control how often the web-based manager updates the display.

More frequent updates use system resources and increase network traffic. However, this only occurs when you are viewing the display using the web-based manager.

4 Select Refresh to manually update the information displayed.

Figure 2: Sessions and network status monitor



Viewing virus and intrusions status

Use the virus and intrusions status display to track when viruses are found by the FortiGate antivirus system and to track when the NIDS detects a network-based attack.

To view virus and intrusions status

1 Go to **System > Status > Monitor**.

2 Select Virus & Intrusions.

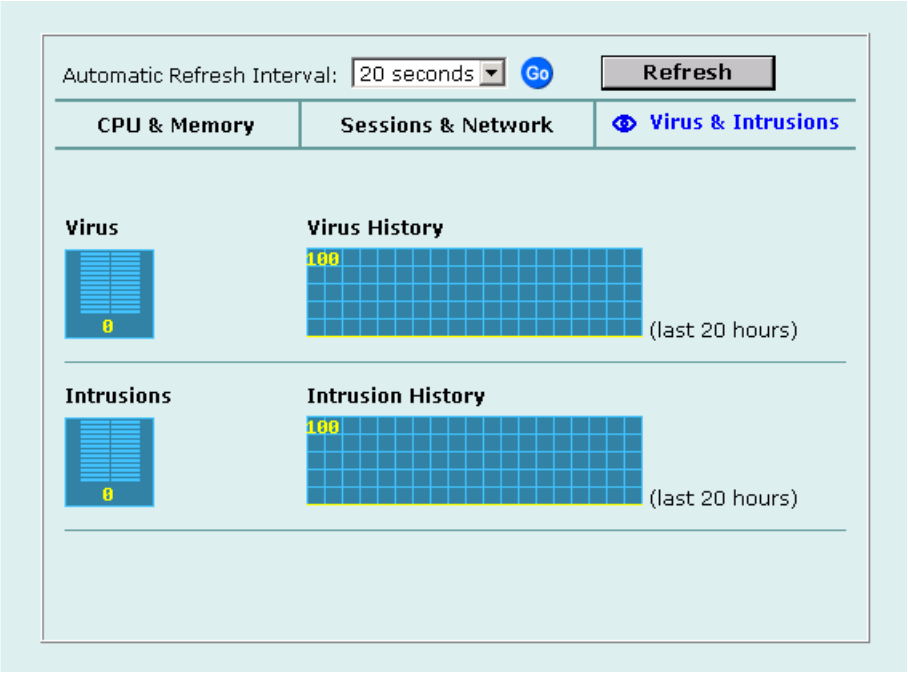
Virus and intrusions status is displayed. The display includes bar graphs of the number viruses and intrusions detected per hour as well as line graphs of the number of viruses and intrusions detected for the last 20 hours.

3 Set the automatic refresh interval and select Go to control how often the web-based manager updates the display.

More frequent updates use system resources and increase network traffic. However, this only occurs when you are viewing the display using the web-based manager. The line graph scales are shown on the upper right corner of the graph.

4 Select Refresh to manually update the information displayed.

Figure 3: Sessions and network status monitor



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. FortiGate administrators with read and write permission and the FortiGate admin user can also stop active communication sessions.

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 Clear to stop an active session.

Each line of the session list displays the following information.

Protocol The service protocol of the connection, for example, udp, tcp, or icmp.
From IP The source IP address of the connection.
From Port The source port of the connection.
To IP The destination IP address of the connection.
To Port The destination port of the connection.
Expire The time, in seconds, before the connection expires.
Clear Stop an active communication session.

Figure 4: Example session list

Total Number of Sessions: 659

Protocol	From IP	From Port	To IP	To Port	Expire (secs)	Clear
udp	192.168.110.200	1242	206.191.0.210	53	76	
tcp	192.168.110.121	4704	192.168.110.3	443	8	
tcp	192.168.110.200	1250	65.39.139.188	110	42	
tcp	192.168.110.121	4699	192.168.110.3	443	8	
tcp	192.168.110.121	4691	192.168.110.3	443	56	
tcp	192.168.110.121	4479	10.0.1.128	6969	72	
udp	192.168.110.200	1246	209.87.239.20	53	86	
udp	192.168.110.200	1246	209.87.239.21	53	89	
tcp	192.168.110.121	4674	192.168.110.3	443	8	
tcp	192.168.110.155	1107	65.39.139.188	143	3262	
tcp	192.168.110.200	1248	65.39.139.188	110	30	
tcp	192.168.110.123	2307	65.39.139.188	110	26	
tcp	192.168.110.121	4701	192.168.110.3	443	8	
tcp	192.168.110.154	1117	65.39.139.188	143	962	
tcp	192.168.110.121	4361	10.0.1.128	6969	49	
tcp	192.168.110.123	2308	65.39.139.188	110	85	
tcp	192.168.110.121	4708	192.168.110.3	443	58	

Virus and attack definitions updates and registration

You can configure the FortiGate unit to connect to the FortiResponse Distribution Network (FDN) to update the antivirus and attack definitions and the antivirus engine. You have the following update options:

- Request updates from the FDN,
- Schedule updates to automatically request the latest versions hourly, daily, or weekly,
- Set Push updates so that the FDN contacts your FortiGate unit when a new update is available.

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

This chapter describes:

Updating antivirus and attack definitions

You can configure the FortiGate unit to connect to the FortiResponse Distribution Network (FDN) to automatically receive the latest antivirus and attack definitions and antivirus engine updates. 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.

The Update page on the web-based manager displays the following antivirus and attack definition update information.

Version	Current antivirus engine, virus definition, and attack definition version numbers.
Expiry date	Expiry date of your license for antivirus engine, virus definition, and attack definition updates.
Last update attempt	Date and time on which the FortiGate unit last attempted to download antivirus engine, virus definition, and attack definition updates.
Last update status	Success or failure 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.

This section describes:

- Connecting to the FortiResponse Distribution Network
- Manually initiating antivirus and attack definitions updates
- Configuring update logging

Connecting to the FortiResponse Distribution Network

Before the FortiGate unit can receive antivirus and attack updates, it must be able to connect to the FortiResponse Distribution Network (FDN). The FortiGate unit uses HTTPS on port 8890 to connect to the FDN. The FortiGate external interface must have a path to the Internet using port 8890. For information about configuring scheduled updates, see “Scheduling updates” on page 76.

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 have a path to the FortiGate external interface using UDP port 9443. For information about configuring push updates, see “Enabling push updates” on page 78.

The FDN is a world-wide network of FortiResponse 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. To make sure the FortiGate unit receives updates from the nearest FDS, check that you have selected the correct time zone for your area.

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 > Update**.
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.

Table 1: Connections to the FDN

Connections	Status	Comments
FortiResponse Distribution Network	Available	The FortiGate unit can connect to the FDN. You can configure the FortiGate unit for scheduled updates. See "Scheduling updates" on page 76.
	Not available	The FortiGate unit cannot connect to the FDN. You must configure your FortiGate unit and your network so that the FortiGate unit can connect to the Internet and to the FDN. 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 FortiResponse server to receive updates. See "Adding an override server" on page 77.
Push Update	Available	The FDN can connect to the FortiGate unit to send push updates. You can configure the FortiGate unit to receive push updates. See "Enabling push updates" on page 78.
	Not available	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 "Registering the FortiGate unit" on page 85), if there is a NAT device installed between the FortiGate unit and the FDN (see "Enabling push updates through a NAT device" on page 79), or if your FortiGate unit connects to the Internet using a proxy server (see "Enabling scheduled updates through a proxy server" on page 78).

Manually initiating antivirus and attack definitions updates

You can use the following procedure to update the antivirus and attack definitions at any time. The FortiGate unit must be able to connect to the FDN or to an override FortiResponse server.

To update antivirus and attack definitions

1 Go to **System > Update**.

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

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 page lists new version information for antivirus definitions, the antivirus engine, or attack definitions. 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.

Configuring update logging

Use the following procedure to configure FortiGate logging to record log messages when the FortiGate unit updates antivirus and attack definitions. The update log messages are recorded on the FortiGate Event log.

To configure update logging

1 Go to **Log&Report > Log Setting**.

2 Select Config Policy for the type of logs that the FortiGate unit is configured to record. For information about recording logs, see "Recording logs" on page 251.

3 Select Update to record log messages when the FortiGate unit updates antivirus and attack definitions.

4 Select any of the following update log options.

Failed Update	Records a log message whenever an update attempt fails.
Successful Update	Records a log message whenever an update attempt is successful.
FDN error	Records a log message whenever it cannot connect to the FDN or whenever it receives an error message from the FDN.

5 Select OK.

Scheduling updates

The FortiGate unit can check for and download updated definitions hourly, daily, or weekly, according to a schedule that you specify.

This section describes:

- Enabling scheduled updates
- Adding an override server
- Enabling scheduled updates through a proxy server

Enabling scheduled updates

To enable scheduled updates

1 Go to **System > Update**.

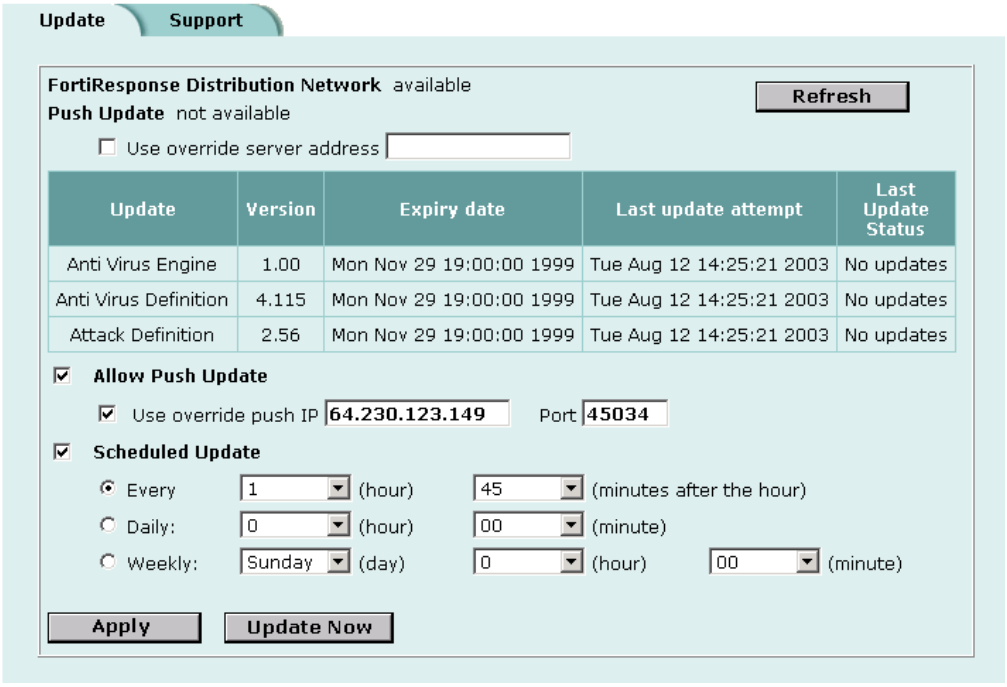
2 Select the Scheduled Update check box.

3 Select one of the following to check for and download updates.

Hourly	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.

Figure 1: Configuring automatic antivirus and attack definitions updates



Adding an override server

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

To add an override server

1 Go to **System > Update**.

2 Select the Use override server address check box.

3 Type the IP address of a FortiResponse server.

4 Select Apply.
The FortiGate unit tests the connection to the override server.

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

If the FortiResponse 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 connecting to the override FortiResponse server.

Enabling scheduled updates through a proxy server

If your FortiGate unit must connect to the Internet through a proxy server, you can use the `set 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:

```
set system autoupdate tunneling enable [address
<proxy-address_ip> [port <proxy-port> [username <username_str>
[password <password_str>]]]]
```

For example, if the IP address of the proxy server is 64.23.6.89 and its port is 8080, enter the following command:

```
set system autouopdate tunneling enable address 64.23.6.89
port 8080
```

For more information about the `set system autoupdate` command, see *Volume 6, 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 “Registering the FortiGate unit” on page 85.

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, or new attack definitions 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 “Enabling scheduled updates through a proxy server” on page 78.

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.

This section describes:

Enabling push updates

To enable push updates

1. Go to **System > Update**.
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 79.

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.

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.

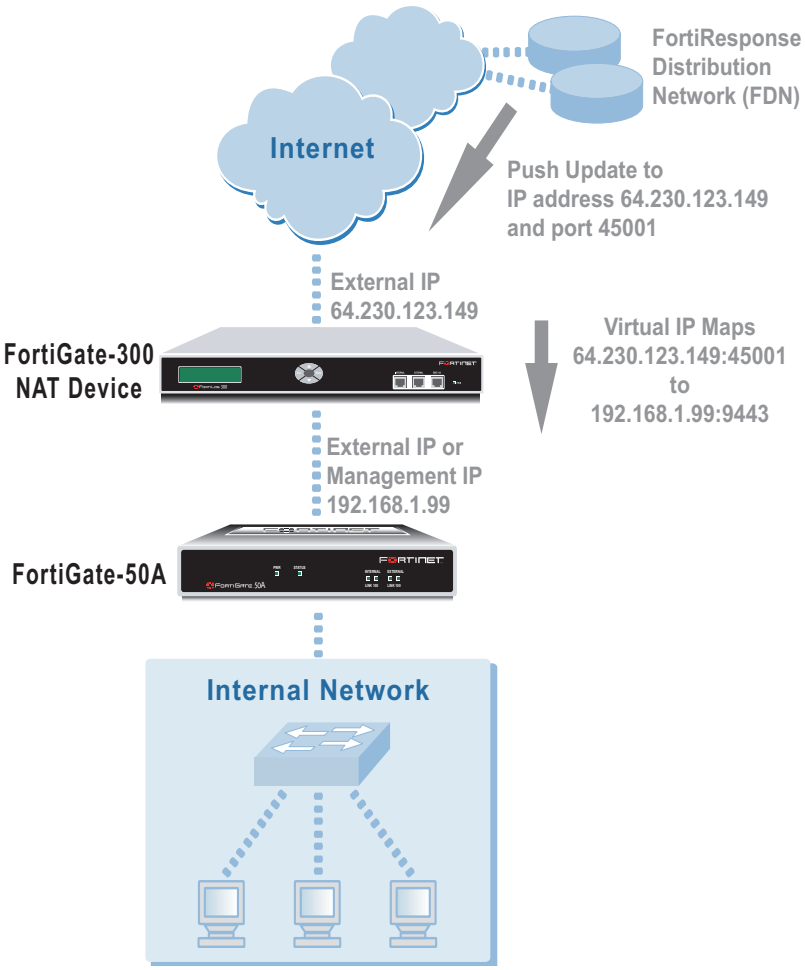
Note: You cannot receive push updates through a NAT device if the external IP address of the NAT device is dynamic (for example, set using PPPoE or DHCP).

Example: push updates through a NAT device

This example describes how to configure a FortiGate NAT device to forward push updates to a FortiGate unit installed on its internal network. For the FortiGate unit on the internal network to receive push updates, the FortiGate NAT device must be configured with a port forwarding virtual IP. This virtual IP maps the IP address of the external interface of the FortiGate NAT device and a custom port to the IP address of the FortiGate unit on the internal network. This IP address can either be the external IP address of the FortiGate unit if it is operating in NAT/Route mode, or the Management IP address of the FortiGate unit if it is operating in Transparent mode.

Note: This example describes the configuration for a FortiGate NAT device. However, you can use any NAT device with a static external IP address that can be configured for port forwarding.

Figure 2: Example network topology: Push updates through a NAT device



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.

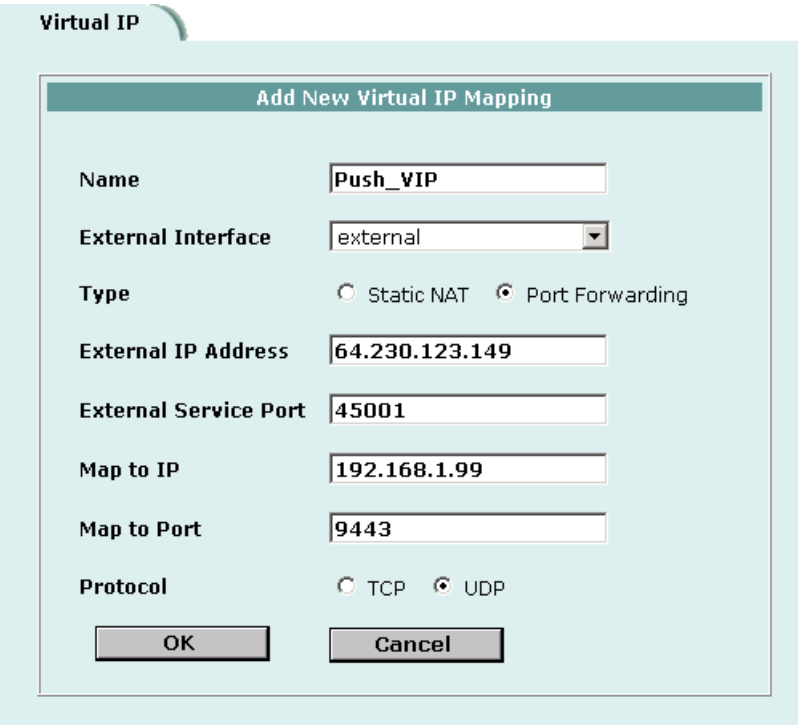
Adding a port forwarding virtual IP to the FortiGate NAT device

Use the following procedure to 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.

To configure the FortiGate NAT device

1. Go to **Firewall > Virtual IP**.
2. Select New.
3. Type a name for the virtual IP.
4. In the External Interface section, select the external interface that the FDN connects to.
   For the example topology, select the external interface.
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.
   For the example topology, enter 64.230.123.149.
7. Type the External Service Port that the FDN connects to.
   For the example topology, enter 45001.
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.
   For the example topology, enter 192.168.1.99.
9. Set the Map to Port to 9443.
10. Set Protocol to UDP.
11. Select OK.

Figure 3: Push update port forwarding virtual IP



Adding a firewall policy for the port forwarding virtual IP

To configure the FortiGate NAT device

1 Add a new external to internal firewall policy.

2 Configure the policy with the following settings:

Source	External_All
Destination	The virtual IP added above.
Schedule	Always
Service	ANY
Action	Accept
NAT	Selected.

3 Select OK.

Configuring the FortiGate unit with an override push IP and port

To configure the FortiGate unit on the internal network

1 Go to **System > Update**.

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.

For the example topology, enter 64.230.123.149.

5 Set Port to the external service port added to the virtual IP.

For the example topology, enter 45001.

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 change, add the changes to the Use override push configuration and select Apply to update the push information on the FDN.

Figure 4: Example push update configuration

7 Select Apply.

8 You can select Refresh to make sure that push updates work.

Push Update changes to Available.

Registering FortiGate units

After purchasing and installing a new FortiGate unit, you can register the unit using the web-based manager by going to 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.

This section describes:

FortiCare Service Contracts

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.

Registering the 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.

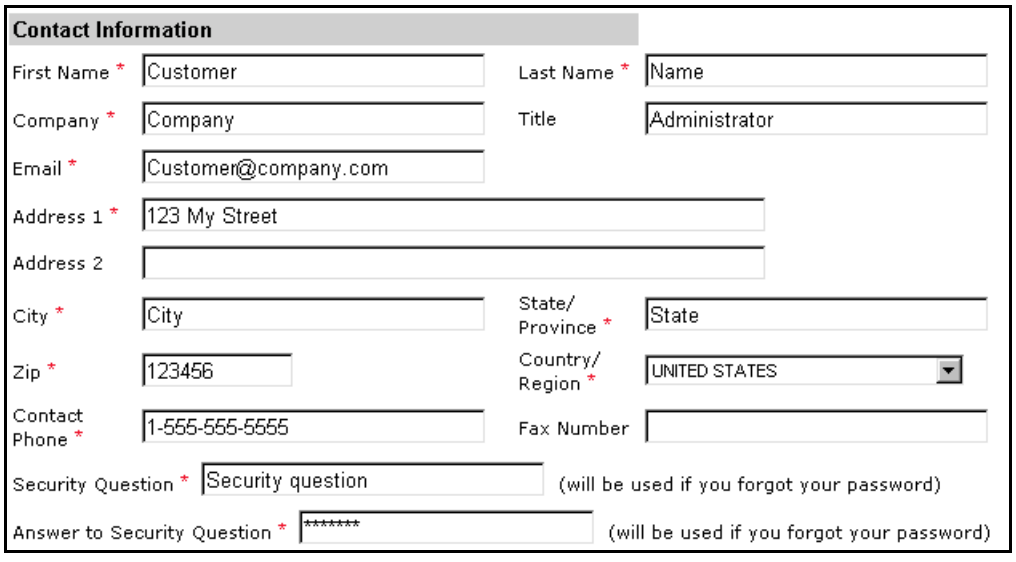
  The serial number is also available from the CLI using the `get system status` command.
- FortiCare Support Contract numbers, if you purchased FortiCare Support Contracts for the FortiGate units that you want to register.

To register one or more FortiGate units

1 Go to **System > Update > Support**.

2 Enter your contact information on the product registration form.

Figure 5: Registering a FortiGate unit (contact information and security question)



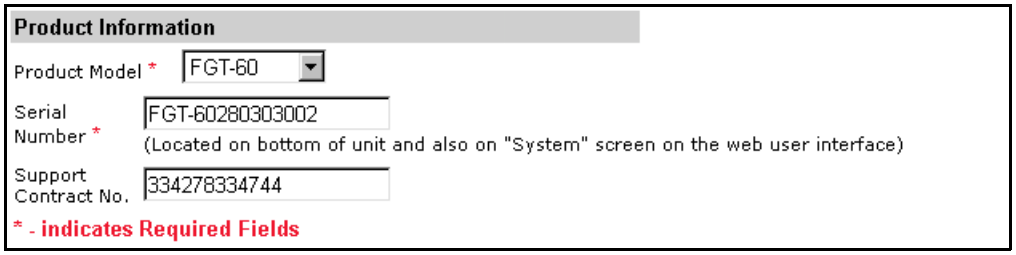
3 Provide a security question and an answer to the security question.

4 Select the model number of the Product Model to register.

5 Enter the Serial Number of the FortiGate unit.

6 If you have purchased a FortiCare Support Contract for this FortiGate unit, enter the support contract number.

Figure 6: Registering a FortiGate unit (product information)



7 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.

Your Fortinet support user name and password is sent to the email address provided with your contact information.

Updating registration information

You can use your Fortinet support user name and password to log on to the Fortinet Support web site at any time to view or update your Fortinet support information.

This section describes:

- Recovering a lost Fortinet support password
- Viewing the list of registered FortiGate units
- Registering a new FortiGate unit
- Adding or changing a FortiCare Support Contract number
- Changing your Fortinet support password
- Changing your contact information or security question
- Downloading virus and attack definitions updates

Recovering a lost Fortinet support password

If you provided a security question and answer when you registered on the Fortinet support web site, you can use the following procedure to receive a replacement password. If you did not provide a security question and answer, contact Fortinet technical support.

To recover a lost Fortinet support password

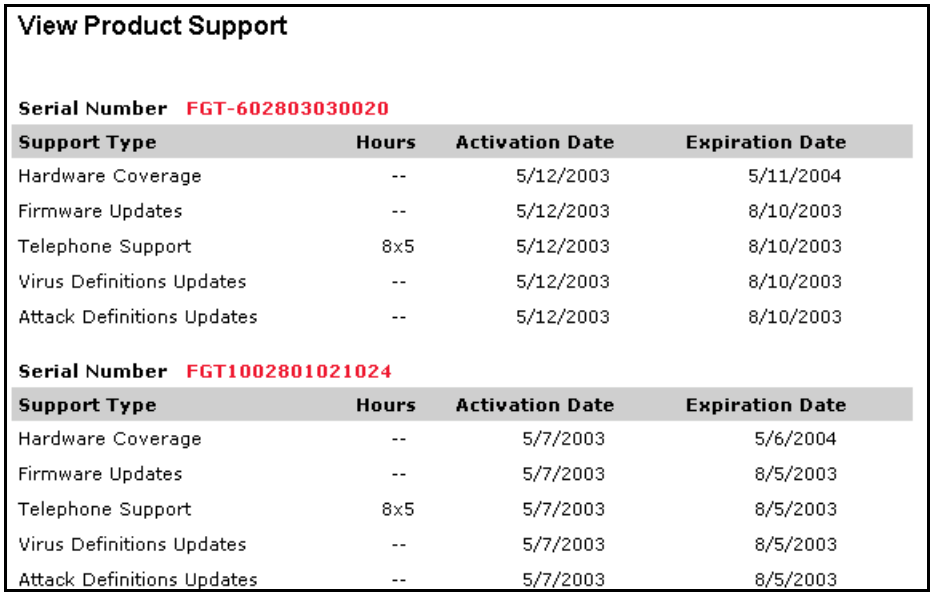
1. Go to **System > Update > Support**.
2. Select Support Login.
3. Enter your Fortinet support user name.
4. Select Forgot your password?
5. Enter your email address and select Submit.
   The security question that you entered when you registered is displayed.
6. Enter the answer to your security question and select Get Password.
   If you entered the correct answer to the security question, an email containing a new password is sent to your email address. You can use your current user name and this password to log into the Fortinet support web site.
7. Select Support Login.
8. When you receive your new password, enter your user name and new password to log into the Fortinet support web site.

Viewing the list of registered FortiGate units

To view the list of registered FortiGate units

1. Go to **System > Update > Support**.
2. Select Support Login.
3. Enter your Fortinet support user name and password.
4. Select Login.
5. Select View Products.
   The list of FortiGate products that you have registered is displayed. For each FortiGate unit, the list includes the serial number and current support options for that unit.

Figure 7: Sample list of registered FortiGate units



View Product Support

Serial Number FGT-602803030020

Support Type	Hours	Activation Date	Expiration Date
Hardware Coverage	--	5/12/2003	5/11/2004
Firmware Updates	--	5/12/2003	8/10/2003
Telephone Support	8x5	5/12/2003	8/10/2003
Virus Definitions Updates	--	5/12/2003	8/10/2003
Attack Definitions Updates	--	5/12/2003	8/10/2003

Serial Number FGT1002801021024

Support Type	Hours	Activation Date	Expiration Date
Hardware Coverage	--	5/7/2003	5/6/2004
Firmware Updates	--	5/7/2003	8/5/2003
Telephone Support	8x5	5/7/2003	8/5/2003
Virus Definitions Updates	--	5/7/2003	8/5/2003
Attack Definitions Updates	--	5/7/2003	8/5/2003

Registering a new FortiGate unit

To register a new FortiGate unit

1. Go to **System > Update > Support**.
2. Select Support Login.
3. Enter your Fortinet support user name and password.
4. Select Login.
5. Select Add Registration.
6. Select the model number of the product model that you want to register.
7. Enter the serial number of the FortiGate unit.
8. If you have purchased a FortiCare Support Contract for this FortiGate unit, enter the support contract number.
9. Select Finish.

   The list of FortiGate products that you have registered is displayed. The list now includes the new FortiGate unit.

Adding or changing a FortiCare Support Contract number

To add or change a FortiCare Support Contract number

1. Go to **System > Update > Support**.
2. Select Support Login.
3. Enter your Fortinet support user name and password.
4. Select Login.
5. Select Add/Change Contract number.

6 Select the Serial Number of the FortiGate unit for which to add or change a FortiCare Support Contract number.

7 Add the new Support Contract number.

8 Select Finish.

The list of FortiGate products that you have registered is displayed. The list now includes the new support contract information.

Changing your Fortinet support password

To change your Fortinet support password

1 Go to **System > Update > Support**.

2 Select Support Login.

3 Enter your Fortinet support user name and password.

4 Select Login.

5 Select My Profile.

6 Select Change Password.

7 Enter your current password.

8 Enter and confirm a new password.

An email is sent to your email address confirming that your password has been changed. Use your current user name and new password the next time you log into the Fortinet technical support web site.

Changing your contact information or security question

To change your contact information or security question

1 Go to **System > Update > Support**.

2 Select Support Login.

3 Enter your Fortinet support user name and password.

4 Select Login.

5 Select My Profile.

6 Select Edit Profile.

7 Make the required changes to your contact information.

8 Make the required changes to your security question and answer.

9 Select Update Profile.

Your changes are saved to the Fortinet technical support database. If you changed your contact information, the changes are displayed.

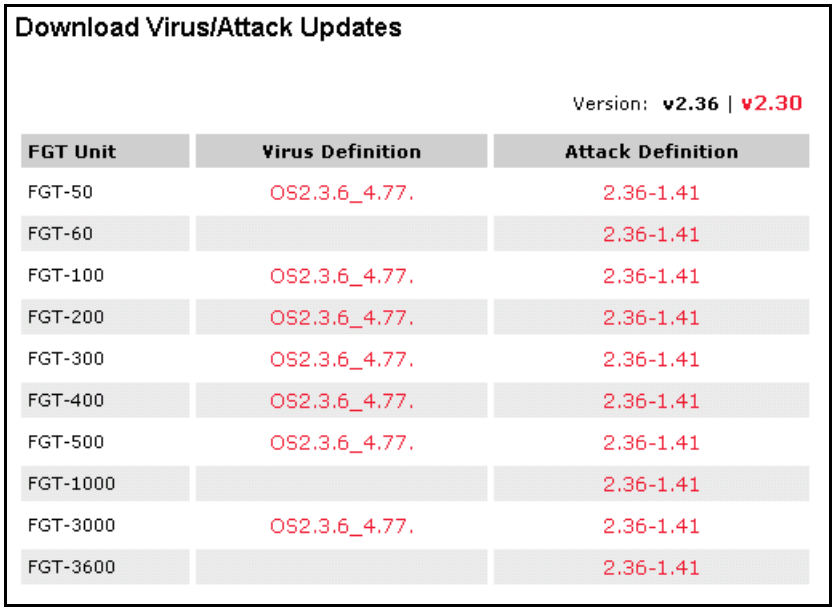
Downloading virus and attack definitions updates

Use the following procedure to manually download virus and attack definitions updates. This procedure also describes how to install the attack definitions updates on your FortiGate unit.

To download virus and attack definitions updates

1. Go to **System > Update > Support**.
2. Select Support Login.
3. Enter your Fortinet support user name and password.
4. Select Login.
5. Select Download Virus/Attack Update.
6. If required, select the FortiOS version.
7. Select the virus and attack definitions to download.

Figure 8: Downloading virus and attack definition updates


Download Virus/Attack Updates

Version: v2.36 | v2.30

FGT Unit	Virus Definition	Attack Definition
FGT-50	OS2.3.6_4.77.	2.36-1.41
FGT-60		2.36-1.41
FGT-100	OS2.3.6_4.77.	2.36-1.41
FGT-200	OS2.3.6_4.77.	2.36-1.41
FGT-300	OS2.3.6_4.77.	2.36-1.41
FGT-400	OS2.3.6_4.77.	2.36-1.41
FGT-500	OS2.3.6_4.77.	2.36-1.41
FGT-1000		2.36-1.41
FGT-3000	OS2.3.6_4.77.	2.36-1.41
FGT-3600		2.36-1.41

For information about how to install the downloaded files, see “Manual virus definition updates” on page 63 and “Manual attack definition updates” on page 63.

Registering a FortiGate unit after an RMA

The Return Material Authorization (RMA) process starts when a registered FortiGate unit does not work properly because of a hardware failure. If this happens while the FortiGate unit is protected by hardware coverage, you can return the FortiGate unit that is not functioning to your reseller or distributor.

The RMA is recorded and you will receive a replacement unit. Fortinet adds the RMA information to the Fortinet support database. When you receive the replacement unit you can use the following procedure to update your product registration information.

To register a FortiGate unit after an RMA

1. Go to **System > Update > Support**.
2. Select Support Login.
3. Enter your Fortinet support user name and password to log in.
4. Select Add Registration.
5. Select the link to replace a unit with a new unit from an RMA.
6. Select Finish.

   The list of FortiGate products that you have registered is displayed. The list now includes the replacement FortiGate unit. All support levels are transferred to the replacement unit.

Network configuration

You can use the System Network page to change any of the following FortiGate network settings:

- Configuring interfaces
- Adding DNS server IP addresses
- Configuring routing
- Configuring DHCP services
- Configuring the modem interface

Configuring interfaces

Use the following procedures to configure FortiGate interfaces:

- Viewing the interface list
- Changing the administrative status of an interface
- Configuring an interface with a manual IP address
- Configuring an interface for DHCP
- Configuring an interface for PPPoE
- Adding a secondary IP address to an interface
- Adding a ping server to an interface
- Controlling administrative access to an interface
- Changing the MTU size to improve network performance
- Configuring traffic logging for connections to an interface
- Configuring the management interface in Transparent mode

Viewing the interface list

To view the interface list

1 Go to **System > Network > Interface**.
The interface list is displayed. The interface list shows the following status information for all the FortiGate interfaces and VLAN subinterfaces:

- The name of the interface
- The IP address of the interface
- The netmask of the interface
- The administrative access configuration for the interface
  See "Controlling administrative access to an interface" on page 97 for information about administrative access options.
- 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 "Changing the administrative status of an interface" on page 94.

Changing the administrative status of an interface

You can use the following procedures to start an interface that is administratively down and stop and interface that is administratively up.

To start up an interface that is administratively down

1 Go to **System > Network > Interface**.
The interface list is displayed.

2 Select Bring Up for the interface that you want to start.

To stop an interface that is administratively up

1 From the FortiGate CLI, enter the command:

```
set system interface <intf_str> config status down
```

You can only stop an interface that is administratively up from the FortiGate command line interface (CLI).

Configuring an interface with a manual IP address

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

To change an interface with a manual IP address

1 Go to **System > Network > Interface**.

2 Choose an interface and select Modify  .

3 Set Addressing Mode to Manual.

4 Change the IP address and Netmask as required.

The IP address of the interface must be on the same subnet as the network the interface is connecting to.

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

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.

Configuring an interface for DHCP

You can configure any FortiGate interface to use 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.

By default, the FortiGate unit also retrieves a default gateway IP address and DNS server IP addresses from the DHCP server. You can disable the option Retrieve default gateway and DNS from server if you do not want the DHCP server to configure these FortiGate settings.

To configure an interface for DHCP

1 Go to **System > Network > Interface**.

2 Choose an interface and select Modify  .

3 In the Addressing Mode section, select DHCP.

4 Clear the Retrieve default gateway and DNS from server check box if you do not want the FortiGate unit to obtain a default gateway IP address and DNS server IP addresses from the DHCP server.

By default, this option is enabled.

5 Clear the Connect to Server check box if you do not want the FortiGate unit to connect to the DHCP server.

By default, this option is enabled.

6 Select Apply.

The FortiGate unit attempts to contact the DHCP server from the interface to set the IP address, netmask, default gateway IP address, and DNS server IP addresses.

7 Select Status to refresh the addressing mode status message.

initializing	No activity
connecting	The FortiGate unit is attempting to connect to the DHCP server.
connected	The FortiGate unit retrieves an IP address, netmask, and other settings from the DHCP server.
failed	The FortiGate unit was unable to retrieve an IP address and other information from the DHCP server.

8 Select OK.

Configuring an interface for PPPoE

Use the following procedure to configure any FortiGate interface to use 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.

By default, the FortiGate unit also retrieves a default gateway IP address and DNS server IP addresses from the PPPoE server. You can disable the option Retrieve default gateway and DNS from server if you do not want the PPPoE server to configure these FortiGate settings.

To configure an interface for PPPoE

1. Go to **System > Network > Interface**.
2. Choose an interface and select Modify  .
3. In the Addressing Mode section, select PPPoE.
4. Enter your PPPoE account User Name and Password.
5. Clear the Retrieve default gateway and DNS from server check box if you do not want the FortiGate unit to obtain a default gateway IP address and DNS server IP addresses from the PPPoE server.
   By default, this option is enabled.
6. Clear the Connect to Server check box if you do not want the FortiGate unit to connect to the PPPoE server.
   By default, this option is enabled.
7. Select Apply.
   The FortiGate unit attempts to contact the PPPoE server from the interface to set the IP address, netmask, default gateway IP address, and DNS server IP addresses.
8. Select Status: to refresh the addressing mode status message. Possible messages:

initializing	No activity
connecting	The FortiGate unit is attempting to connect to the DHCP server.
connected	The FortiGate unit retrieves an IP address, netmask, and other settings from the PPPoE server.
failed	The FortiGate unit was unable to retrieve an IP address and other information from the PPPoE server.

9. Select OK.

Adding a secondary IP address to an interface

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.

To add a secondary IP address from the CLI enter the command:

```
set system interface <intf_str> config secip <second_ip>
<netmask_ip>
```

You can also configure management access and add a ping server to the secondary IP address.

```
set system interface <intf_str> config secallowaccess ping
https ssh snmp http telnet
set system interface <intf_str> config secgwdetect enable
```

Adding a ping server to an interface

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 "Adding destination-based routes to the routing table" on page 101.

To add a ping server to an interface

1. Go to **System > Network > Interface**.
2. Choose an interface and select Modify  .
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.
   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 "Modifying the Dead Gateway Detection settings" on page 123.
5. Select OK to save the changes.

Controlling 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 122).

To configure administrative access in Transparent mode, see "Configuring the management interface in Transparent mode" on page 99.

To control administrative access to an interface

1. Go to **System > Network > Interface**.

2 Choose an interface and select Modify  .

3 Select the Administrative Access methods for the interface.

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 125.
TELNET	To allow Telnet connections to the CLI through this interface. Telnet connections are not secure and can be intercepted by a third party.

4 Select OK to save the changes.

Changing the MTU size to improve network performance

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 size of the packets leaving an interface

1 Go to **System > Network > Interface**.

2 Choose an interface and select Modify  .

3 Select Override default MTU value (1500).

4 Set the MTU size.

Set 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.

Configuring traffic logging for connections to an interface

To configure traffic logging for connections to an interface

1 Go to **System > Network > Interface**.

2 Choose an interface and select Modify  .

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.

Configuring the management interface in Transparent mode

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 "Updating antivirus and attack definitions" on page 73).

You can also configure the management interface to control how administrators connect to the FortiGate unit for administration and the FortiGate interfaces to which administrators can connect.

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 122).

To configure the management interface in Transparent mode

1. Go to **System > Network > Management**.
2. Change the Management IP and Netmask as required.
   This must be a valid IP address for the network that you want to manage the FortiGate unit from.
3. Add a default gateway IP address if the FortiGate unit must connect to a default gateway to reach the management computer.
4. Select the administrative access methods for each interface.

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 125.
TELNET	To allow Telnet connections to the CLI through this interface. Telnet connections are not secure and can be intercepted by a third party.

5. Select Log for each interface that you want to record log messages whenever a firewall policy accepts a connection to this interface.
6. Select Apply to save the changes.

Adding DNS server IP addresses

Several FortiGate functions, including sending email alerts and URL blocking, use DNS. Use the following procedure to add the IP addresses of the DNS servers that your FortiGate unit can connect to. DNS server IP addresses are usually supplied by your ISP.

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.

Configuring routing

This section describes how to configure FortiGate routing. You can configure routing to add static routes from the FortiGate unit to local routers. Using policy routing you can increase the flexibility of FortiGate routing to support more advanced routing functions.

You can also use routing to create a multiple Internet connection configuration that supports redundancy and load sharing between the two Internet connections.

This section describes:

- Adding a default route
- Adding destination-based routes to the routing table
- Adding routes in Transparent mode
- Configuring the routing table
- Policy routing

Adding a default route

You can add a default route for network traffic leaving the external interface.

To add a default route

1. Go to **System > Network > Routing Table**.
2. Select New to add a new route.
3. Set the Source IP and Netmask to 0.0.0.0.
4. Set the Destination IP and Netmask to 0.0.0.0.
5. Set Gateway 1 to the IP address of the routing gateway that routes traffic to the Internet.
6. Select OK to save the default route.

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.

Adding destination-based routes to the routing table

You can add destination-based routes to the FortiGate routing table 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.

You can add one or two gateways to a route. If you add one gateway, the FortiGate unit routes the traffic to that gateway. You can add a second gateway to route traffic to the second gateway if the first gateway fails.

To support routing failover, the IP address of each gateway must be added to the ping server of the interface connected to the same network as the gateway. For information about adding a ping server, see "Adding a ping server to an interface" on page 97.

To add destination-based routes to the routing table

1. Go to **System > Network > Routing Table**.
2. Select New to add a new route.
3. Type the Destination IP address and netmask for the route.
4. Add the IP address of Gateway #1.

   Gateway #1 is the IP address of the primary destination for the route.

   Gateway #1 must be on the same subnet as a Fortigate interface.

   If you are adding a static route from the FortiGate unit to a single destination router, you need to specify only one gateway.
5. Add the IP address of Gateway #2, if you want to route traffic to multiple gateways.
6. Set Device #1 to the FortiGate interface through which you want to route traffic to connect to Gateway #1.

   You can select the name of an interface or Auto (the default). If you select the name of an interface, the traffic is routed to that interface. If you select Auto the system selects the interface according to the following rules:

   - If the Gateway #1 IP address is on the same subnet as a FortiGate interface, the system sends the traffic to that interface.
   - If the Gateway #1 IP address is not on the same subnet as a FortiGate interface, the system routes the traffic to the external interface, using the default route.

   You can use Device #1 to send packets to an interface that is on a different subnet than the destination IP address of the packets without routing them using the default route.

7 Set Device #2 to the FortiGate interface through which to route traffic to connect to Gateway #2.

You can select the name of an interface or Auto (the default). If you select the name of an interface, the traffic is routed to that interface. If you select Auto the system selects the interface according to the following rules:

- If the Gateway #2 IP address is on the same subnet as a FortiGate interface, the system sends the traffic to that interface.
- If the Gateway #2 IP address is not on the same subnet as a FortiGate interface, the system routes the traffic to the external interface, using the default route.

You can use Device #2 to send packets to an interface that is on a different subnet than the destination IP address of the packets without routing them using the default route.

8 Select OK to save the route.

Note: Any two routes in the routing table must differ by something other than just the gateway to be simultaneously active. If two routes added to the routing table are identical except for their gateway IP addresses, only the route closer to the top of the routing table can be active.

Note: Arrange routes in the routing table from more specific to more general. For information about arranging routes in the routing table, see "Configuring the routing table".

Adding routes in Transparent mode

Use the following procedure to add routes when operating the FortiGate unit in Transparent mode.

To add a route in Transparent mode

1 Go to **System > Network > Routing**.

2 Select New.

3 Enter the Destination IP address and Netmask for the route.

4 Enter the Gateway IP address for the route.

5 Select OK to save the new route.

6 Repeat steps 1 to 5 to add more routes as required.

Configuring the routing table

The routing table shows the destination IP address and mask of each route that you add, as well as the gateways and devices added to the route. The routing table also displays the gateway connection status. A green check mark indicates that the FortiGate unit has used the ping server and dead gateway detection to determine that it can connect to the gateway. A red X means that a connection cannot be established. A blue question mark means that the connection status is unknown. For more information, see "Adding a ping server to an interface" on page 97.

The FortiGate unit assigns routes using a best match algorithm based on the destination address of the packet and the destination address of the route. To select a route for a packet, the FortiGate unit searches 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.

To configure the routing table

1. Go to **System > Network > Routing Table**.
2. Choose the route that you want to move and select Move to to change its order in the routing table.
3. Type a number in the Move to field to specify where in the routing table to move the route and select OK.
4. Select Delete to delete a route from the routing table.

Figure 9: Routing table

Policy routing

Policy routing extends the functions of destination routing. Using policy routing you can route traffic based on the following:

- Destination address
- Source address
- Protocol, service type, or port range
- Incoming or source interface

Using policy routing you can build a routing policy database (RPDB) that selects the appropriate route for traffic by applying a set of routing rules. To select a route for traffic, the FortiGate unit matches the traffic with the policy routes added to the RPDB starting at the top of the list. The first policy route that matches is used to set the route for the traffic. The route supplies the next hop gateway as well as the FortiGate interface to be used by the traffic.

Packets are matched with policy routes before they are matched with destination routes. If a packet does not match a policy route, it is routed using destination routes.

The gateway added to a policy route must also be added to a destination route. When the FortiGate unit matches packets with a route in the RPDB, the FortiGate unit looks in the destination routing table for the gateway that was added to the policy route. If a match is found, the FortiGate unit routes the packet using the matched destination route. If a match is not found, the FortiGate unit routes the packet using normal routing.

To find a route with a matching gateway, the FortiGate unit starts at the top of the destination routing table and searches until it finds the first matching destination route. This matched route is used to route the packet.

Policy routing command syntax

Configure policy routing using the following CLI command.

```
set system route policy <route_int> src <source_ip>
<source_mask> iifname <source-interface_name>
dst <destination_ip> <destination_mask>
oifname <destination-interface_name> protocol <protocol_int>
port <low-port_int> <high-port_int> gw <gateway_ip>
```

Complete policy routing command syntax is described in *Volume 6: FortiGate CLI Reference Guide*.

Configuring DHCP services

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

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

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 the following:

Configuring a DHCP relay agent

In a DHCP relay configuration, the FortiGate unit 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.

To configure an interface as a DHCP relay agent

1. Go to **System > Network > DHCP**.
2. Select Service.
3. Select the interface to be the DHCP relay agent.
4. Select DHCP Relay Agent.
5. Enter the DHCP Server IP address.
6. Select Apply.

Configuring a DHCP server

As a DHCP server, the FortiGate unit dynamically assigns IP addresses to hosts located on connected subnets. You can configure a DHCP server for any FortiGate interface. You can also configure a DHCP server for more than one FortiGate interface. For each DHCP server configuration you can add multiple scopes (also called address scopes) so that the DHCP server can assign IP addresses to computers on multiple subnets.

Use these procedures to configure an interface as a DHCP server:

- Adding a DHCP server to an interface
- Adding scopes to a DHCP server
- Adding a reserve IP to a DHCP server
- Viewing a DHCP server dynamic IP list

Adding a DHCP server to an interface

To add a DHCP server to an interface

1. Go to **System > Network > DHCP**.
2. Select Service.
3. Select an interface.
4. Select DHCP Server.
5. Select Apply.

Adding scopes to a DHCP server

If you have configured an interface as a DHCP server, the interface requires at least one scope (also called an address scope). The scope designates the starting IP and ending IP for the range of addresses that the FortiGate unit assigns to DHCP clients.

You can add multiple scopes to an interface so that the DHCP server added to that interface can supply IP addresses to computers on multiple subnets.

Add multiple scopes if the DHCP server receives DHCP requests from subnets that are not connected directly to the FortiGate unit. In this case, the DHCP requests are sent to the FortiGate unit through DHCP relay. DHCP relay packets contain DHCP relay IP, which is the IP address of the subnet from which the DHCP relay received the request.

If the DHCP request received by the DHCP server is not forwarded by a DHCP relay, the DHCP server decides which scope to use based on the IP address of the interface that received the DHCP request; usually the scope with the same subnet as the interface.

If the DHCP request received by the server is forwarded by a DHCP relay, the relay IP is used to select the scope.

To add a scope to a DHCP server

1. Go to **System > Network > DHCP**.
2. Select Address Scope.

3 Select an interface.
You must configure the interface as a DHCP server before it can be selected.

4 Select New to add an address scope.

5 Configure the address scope.

Scope Name	Enter the address scope name.
IP Pool	Enter the starting IP and ending IP for the range of IP addresses that this DHCP server assigns to DHCP clients.
Netmask	Enter the netmask that the DHCP server assigns to the DHCP clients.
Lease Duration	Enter the interval, in days, hours and minutes, after which a DHCP client must ask the DHCP server for a new address. If you select Unlimited, DHCP leases never expire.
Domain	Optionally enter in the domain that the DHCP server assigns to the DHCP clients.
Default Route	Enter the default route to be assigned to DHCP clients. The default route must be on the same subnet as the IP pool.

6 Select Advanced if you want to configure Advanced Options.

DNS IP	Enter the addresses of up to 3 DNS servers that the DHCP server assigns to the DHCP clients.
WINS Server IP	Add the IP addresses of one or two WINS servers to be assigned to DHCP clients.
Exclusion Range	Optionally enter up to 4 exclusion ranges of IP addresses within the IP pool that cannot be assigned to DHCP clients.

7 Select OK.

Adding a reserve IP to a DHCP server

If you have configured an interface as a DHCP server, you can 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 of a device and an IP address to the reserve IP list, the DHCP server always assigns this IP address to the device.

To add a reserve IP you must first select the interface and scope to which you want to add the reserve IP.

To add a reserve IP to a DHCP server

1 Go to **System > Network > DHCP**.

2 Select Reserve IP.

3 Select an interface.
You must configure the interface as a DHCP server before you can select it.

4 Select a scope.
You must configure an address scope for the interface before you can select it.

5 Select New to add a reserved IP.

6 Configure the reserved IP.

IP	Enter an IP address. The IP address must be within the IP pool added to the selected scope.
MAC	Enter the MAC address of the device.
Name	Optionally, specify a name for the IP and MAC address pair.

Note: The reserved IP cannot be assigned to any other device. You can only add a given IP address or MAC address once.

7 Select OK.

Viewing a DHCP server dynamic IP list

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.

To view a DHCP server dynamic IP list

1 Go to **System > Network > DHCP**.

2 Select Dynamic IP.

3 Select the interface for which you want to view the list.

Configuring the modem interface

You can connect a modem to the FortiGate unit and use it as either a backup interface or standalone interface.

- In backup mode, the modem interface automatically takes over from a selected ethernet interface when that ethernet interface is unavailable.
- In standalone mode, the modem interface is the connection from the FortiGate unit to the Internet.

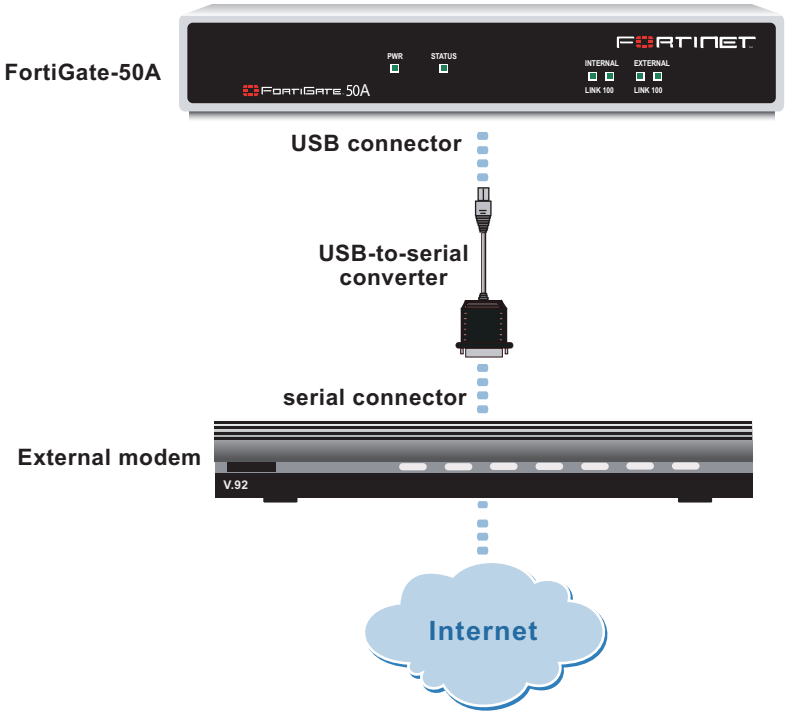
When connecting to the ISP, in either configuration, the FortiGate unit modem can automatically dial up to three dialup accounts until the modem connects to an ISP.

- Connecting a modem to the FortiGate unit
- Configuring modem settings
- Connecting to a dialup account
- Disconnecting the modem
- Viewing modem status
- Backup mode configuration
- Standalone mode configuration
- Adding firewall policies for modem connections

Connecting a modem to the FortiGate unit

The FortiGate unit can operate with most standard external serial interface modems that support standard Hayes AT commands. To connect, install a USB-to-serial converter between one of the two USB ports on the FortiGate unit and the serial port on the modem. The FortiGate unit does not support a direct USB connection between the two devices.

Figure 10: Example modem interface network connection



Configuring modem settings

Configure modem settings so that the FortiGate unit uses the modem to connect to your ISP dialup accounts. You can configure the modem to connect to up to three dialup accounts. You can also enable and disable FortiGate modem support, configure how the modem dials, and select the FortiGate interface that the modem is redundant for.

To configure modem settings

1. Go to **System > Network > Modem**.
2. Select Enable USB Modem.
3. Change any of the following dialup connection settings:

Redial Limit	The maximum number of times (1-10) that the FortiGate unit dials the ISP to restore an active connection on the modem interface. The default redial limit is 1. Select None to allow the modem to never stop redialing.
Holddown Timer	For backup configurations. The time (1-60 seconds) that the FortiGate unit waits before switching from the modem interface to the primary interface, after the primary interface has been restored. The default is 1 second. Configure a higher value if you find the FortiGate unit switching repeatedly between the primary interface and the modem interface.
Redundant for	To associate the modem interface with the ethernet interface that you want to either back up (backup configuration) or replace (standalone configuration).

4 Enter the following Dialup Account 1 settings:

Phone Number	The phone number required to connect to the dialup account. Do not add spaces to the phone number. Make sure to include standard special characters for pauses, country codes, and other functions as required by your modem to connect to your dialup account.
User Name	The user name (maximum 63 characters) sent to the ISP.
Password	The password sent to the ISP.

5 If you have multiple dialup accounts, enter Phone Number, User Name, and Password for Dialup Account 2 and Dialup Account 3.

6 Select Apply.

Connecting to a dialup account

Use the following procedure to connect the modem to a dialup account.

To connect to a dialup account

1 Go to **System > Network > Modem**.

2 Select Enable USB Modem.

3 Make sure there is correct information in one or more Dialup Accounts.

4 Select Apply if you make any configuration changes.

5 Select Dial Up.
The FortiGate unit initiates dialing into each dialup account in turn until the modem connects to an ISP.

Disconnecting the modem

Use the following procedure to disconnect the modem from a dialup account.

To disconnect the modem

1 Go to **System > Network > Modem**.

2 Select Hang Up if you want to disconnect from the dialup account.

Viewing modem status

To view the status of the modem connection go to **System > Network > Modem**.

Modem status is one of the following:

not active	The modem interface is not connected to the ISP.
active	The modem interface is attempting to connect to the ISP, or is connected to the ISP.

A green check mark indicates the active dialup account.

The IP address and netmask assigned to the modem interface appears on the System Network Interface page of the web-based manager.

Backup mode configuration

The modem interface in backup mode backs up a selected ethernet interface. If that ethernet interface disconnects from its network, the modem automatically dials the configured dialup accounts. When the modem connects to a dialup account, the FortiGate unit routes IP packets normally destined for the selected ethernet interface to the modem interface.

The FortiGate unit disconnects the modem interface and switches back to the ethernet interface when the ethernet interface can again connect to its network.

For the FortiGate unit to be able to switch from an ethernet interface to the modem you must select the name of the interface in the modem configuration and configure a ping server for that interface. You must also configure firewall policies for connections between the modem interface and other FortiGate interfaces.

Note: Do not add policies for connections between the modem interface and the interface that the modem is backing up.

To configure backup mode

1. Go to **System > Network > Modem**.
2. From the Redundant for list, select the ethernet interface that you want the modem to back up.
3. Configure other modem settings as required.
   See “Configuring modem settings” on page 108.
4. Configure a ping server for the ethernet interface selected in step 2.
   See “Adding a ping server to an interface” on page 97.
5. Configure firewall policies for connections to the modem interface.
   See “Adding firewall policies for modem connections” on page 111.

Standalone mode configuration

In standalone mode, you manually connect the modem to a dialup account. The modem interface operates as the primary connection to the Internet. The FortiGate unit routes traffic through the modem interface, which remains permanently connected to the dialup account.

If the connection to the dialup account fails, the FortiGate unit redials the modem. The modem redials the number of times specified by the redial limit, or until it connects to a dialup account.

In standalone mode the modem interface replaces the external ethernet interface. When configuring the modem, you must set Redundant for to the name of the ethernet interface that the modem interface replaces. You must also configure firewall policies for connections between the modem interface and other FortiGate interfaces.

Note: Do not add a default route to the ethernet interface that the modem interface replaces.

Note: Do not add firewall policies for connections between the ethernet interface that the modem replaces and other interfaces.

To operate in standalone mode

1. Go to **System > Network > Modem**.
2. From the Redundant for list, select the ethernet interface that the modem is replacing.
3. Configure other modem settings as required.
   See “Configuring modem settings” on page 108.
   Make sure there is correct information in one or more Dialup Accounts.
4. Select Dial Up.
   The FortiGate unit initiates dialing into each dialup account in turn until the modem connects to an ISP.
5. Configure firewall policies for connections to the modem interface.
   See “Adding firewall policies for modem connections” on page 111.

Adding firewall policies for modem connections

The modem interface requires firewall addresses and policies. You can add one or more addresses to the modem interface. For information about adding addresses, see “Adding addresses” on page 147. When you add addresses, the modem interface appears on the policy grid.

You can configure firewall policies to control the flow of packets between the modem interface and the other interfaces on the FortiGate unit. For information about adding firewall policies, see “Adding firewall policies” on page 140.

RIP configuration

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.

This chapter describes how to configure FortiGate RIP:

RIP settings

To configure RIP on the FortiGate unit

1 Go to **System > RIP > Settings**.

2 Select Enable RIP.

When you enable RIP, the Fortigate unit starts the RIP process. The FortiGate unit does not send or receive RIP packets until you enable RIP on at least one interface. For information about configuring RIP, see “Configuring RIP for FortiGate interfaces” on page 115.

3 Select Enable Advertise Default if you want RIP to always send the default route to neighbors whether or not the default route is in the static routing table.

If you disable Advertise Default, RIP never sends the default route.

4 Change the following RIP default settings, as required.

RIP defaults are effective in most configurations. You should only have to change these settings to troubleshoot problems with the RIP configuration.

Default Metric RIP uses the default metric to advertise routes learned from other routing protocols. Set Default Metric to a positive integer lower than 16 to advertise that metric for all routes learned from other routing protocols. The default setting for the Default Metric is 2.

Input Queue Change the depth of the RIP input queue. The higher the number, the deeper the input queue. Change the input queue depth to prevent loss of information from the routing table when you have a FortiGate unit sending at high speed to a router that cannot receive at high speed. The range is 0 to 1024. The default input queue depth is 50. A queue size of 0 means there is no input queue.

Output Delay Add a delay in milliseconds between packets in a multiple-packet RIP update. Add an output delay if you are configuring RIP on a FortiGate unit that could be sending packets to a router that cannot receive the packets at the rate the FortiGate unit is sending them. Output Delay can be from 8 to 50 milliseconds. The default output delay is 0 milliseconds.

5 Change the following RIP timer settings, as required.

RIP timer defaults are effective in most configurations. You should only have to change these timers to troubleshoot network routing problems. All routers and access servers in the network should have the same RIP timer settings.

Update The time interval in seconds between RIP updates. The default is 30 seconds.

Invalid The time interval in seconds after which a route is declared invalid. Invalid should be at least three times the value of Update.

During the invalid interval, after the first update is missed and before the invalid timer expires, the route is marked inaccessible and advertised as unreachable; however, the route is still used for forwarding packets. The invalid interval allows for the loss of one or more update packets before RIP considers the route unusable. If RIP receives an update for a route, before the invalid timer expires, it resets the invalid timer to 0. The default for Invalid is 180 seconds.

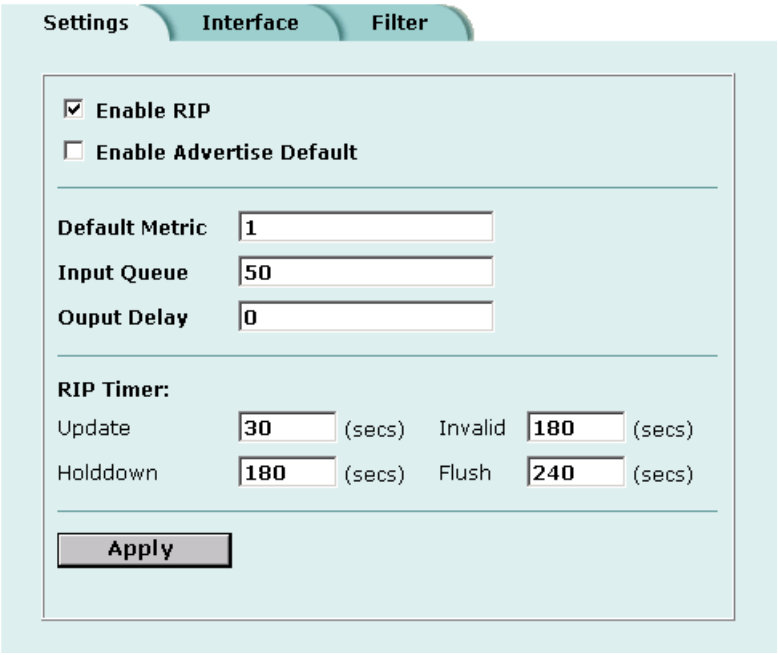
Holddown The time interval in seconds during which RIP ignores routing information for a route. Holddown should be at least three times the value Update.

A route enters the holddown state when RIP receives an update packet indicating that a route is unreachable or when the invalid timer for the route expires. The holddown interval allows time for bad routing information to clear the network during network convergence. The route is marked inaccessible and advertised as unreachable and is no longer used for forwarding packets. The default for Holddown is 180 seconds.

Flush The time in seconds that must elapse after the last update for a route before RIP removes the route from the routing table. Flush should be greater than the value of Invalid to allow the route to go into the holddown state. The default for Flush is 240 seconds.

6 Select Apply to save the changes.

Figure 1: Configuring RIP settings



Configuring RIP for FortiGate interfaces

You can customize a RIP configuration for each FortiGate interface. This allows you to customize RIP for the network to which each interface is connected.

To configure RIP for FortiGate interfaces

1 Go to **System > RIP > Interface**.
On this page you can view a summary of the RIP settings for each FortiGate interface.

2 Select Modify for the interface for which to configure RIP settings.

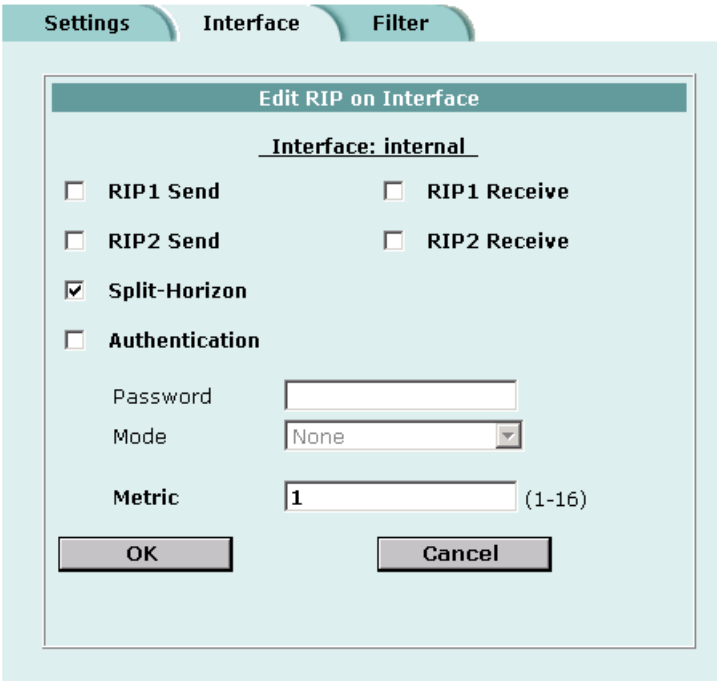
3 Configure any of the following RIP settings:

RIP1 Send	Enables sending RIP version 1 broadcasts from this interface to the network it is connected to. The routing broadcasts are UDP packets with a destination port of 520.
RIP1 Receive	Enables listening on port 520 of an interface for RIP version 1 broadcasts.
RIP2 Send	Enables sending RIP version 2 broadcasts from this interface to the network it is connected to. The routing broadcasts are UDP packets with a destination port of 520.
RIP2 Receive	Enables listening on port 520 of an interface for RIP version 2 broadcasts.
Split-Horizon	Prevents RIP from sending updates for a route back out the interface from which it received those routes. Split horizon is enabled by default. You should only disable split horizon if there is no possibility of creating a counting to infinity loop when network topology changes.
Authentication	Enables authentication for RIP version 2 packets sent and received by an interface. Because the original RIP standard does not support authentication, authentication is only available for RIP version 2.

Password	Enter the password to be used for RIP version 2 authentication. The password can be up to 16 characters long.
Mode	Defines the authentication used for RIP version 2 packets sent and received by this interface. If you select Clear, the password is sent as plain text. If you select MD5, the password is used to generate an MD5 hash. MD5 only guarantees the authenticity of the update packet, not the confidentiality of the routing information in the packet.
Metric	Changes the metric for routes sent by this interface. All routes sent from this interface have this metric added to their current metric value. You can change the interface metric to give a higher priority to an interface. For example, if you have two interfaces that can be used to route packets to the same destination, and you set the metric of one interface higher than the other, the routes to the interface with the lower metric will seem to have a lower cost. More traffic will use routes to the interface with the lower metric. Metric can be from 1 to 16 with 16 equalling unreachable.

4 Select OK to save the RIP configuration for the selected interface.

Figure 2: Example RIP configuration for an internal interface



Adding RIP filters

Use the Filter page to create RIP filter lists and assign RIP filter lists to the neighbors filter, incoming route filter, or outgoing route filter. The neighbors filter allows or denies updates from other routers. The incoming filter accepts or rejects routes in an incoming RIP update packet. The outgoing filter allows or denies adding routes to outgoing RIP update packets.

Each entry in a RIP filter list consists of a prefix (IP address and netmask), the action RIP should take for this prefix (allow or deny), and the interface to which to apply this RIP filter list entry. When RIP applies a filter while processing an update packet, it starts at the top of the filter list and works down through the list looking for a matching prefix. If RIP finds a matching prefix, it then checks that the interface in the filter list entry matches the interface that the packet is received or sent on. If both prefix and interface match, RIP takes the action specified. If no match is found, the default action is allow.

- For the neighbors filter, RIP attempts to match prefixes in the filter list against the source address in the update packet.
- For the incoming filter, RIP attempts to match prefixes in the filter list against prefixes in the routing table entries in the update packet.
- For the outgoing filter, RIP attempts to match prefixes in the filter list against prefixes in the RIP routing table.

You can add up to four RIP filter lists to the FortiGate RIP configuration. You can then select one RIP filter list for each RIP filter type: neighbors, incoming routes, outgoing routes. If you do not select a RIP filter list for any of the RIP filter types, no filtering is applied.

Note: To block all updates not specifically allowed in a filter list, create an entry at the bottom of the filter list with a prefix with 0.0.0.0 for the IP address, 0.0.0.0 for the netmask, and action set to deny. Because RIP uses the first match it finds in a top down search of the filter list, all the allowed entries are matched first, and all other entries for the specified interface are matched by the last entry and denied. Create a separate entry at the bottom of the filter list for each interface for which you want to deny all updates not specifically allowed.

This section describes:

Adding a RIP filter list

Each entry in a RIP filter list consists of a prefix (IP address and netmask), the action RIP should take for this prefix (allow or deny), and the interface to which to apply this RIP filter list entry.

To add a RIP filter list

1. Go to **System > RIP > Filter**.
2. Select New to add a RIP filter.

3 For Filter Name, type a name for the RIP filter list.

The name can be 15 characters long and can contain upper and lower case letters, numbers, and special characters. The name cannot contain spaces.

4 Select the Blank Filter check box to create a RIP filter list with no entries, or enter the information for the first entry on the RIP filter list.

5 Enter the IP address and Mask to create the prefix.

6 For Action, select allow or deny.

7 For Interface, enter the name of the interface to which to apply the entry.

8 Select OK to save the RIP filter list.

To add an entry to a RIP filter list

1 Go to **System > RIP > Filter**.

2 For the RIP filter list name, select ⊞ Add Prefix to add an entry to the filter list.

3 Enter the IP address and Mask to create the prefix.

4 For Action, select allow or deny.

5 For Interface, enter the name of the interface to which to apply the entry.

6 Select OK to add the entry to the RIP filter list.

7 Repeat steps 2 to 6 to add entries to the RIP filter list.

Assigning a RIP filter list to the neighbors filter

The neighbors filter allows or denies updates from other routers. You can assign a single RIP filter list to the neighbors filter.

To assign a RIP filter list to the neighbors filter

1 Go to **System > RIP > Filter**.

2 Add RIP filter lists as required.

3 For Neighbors Filter, select the name of the RIP filter list to assign to the neighbors filter.

4 Select Apply.

Assigning a RIP filter list to the incoming filter

The incoming filter accepts or rejects routes in an incoming RIP update packet. You can assign a single RIP filter list to the incoming filter.

To assign a RIP filter list to the incoming filter

1 Go to **System > RIP > Filter**.

2 Add RIP filter lists as required.

3 For Incoming Routes Filter, select the name of the RIP filter list to assign to the incoming filter.

4 Select Apply.

Assigning a RIP filter list to the outgoing filter

The outgoing filter allows or denies adding routes to outgoing RIP update packets. You can assign a single RIP filter list to the outgoing filter.

To assign a RIP filter list to the outgoing filter

1. Go to **System > RIP > Filter**.
2. Add RIP filter lists as required.
3. For Outgoing Routes Filter, select the name of the RIP filter list to assign to the outgoing filter.
4. Select Apply.

System configuration

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

- Setting system date and time
- Changing system options
- Adding and editing administrator accounts
- Configuring SNMP
- Replacement messages

Setting system date and 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.

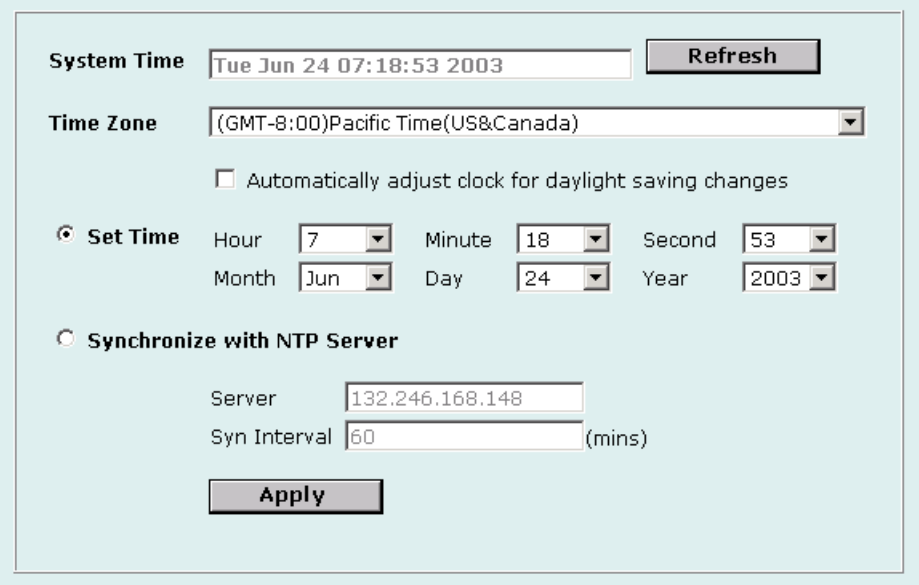
To set the date and time

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. 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.
5. Select Set Time and set the FortiGate system date and time to the correct date and time, if required.
6. Select Synchronize with NTP Server to configure the FortiGate unit to use NTP to automatically set the system time and date.

   For more information about NTP and to find the IP address of an NTP server that you can use, see http://www.ntp.org.
7. Enter the IP address or domain name of the NTP server that the FortiGate unit can use to set its time and date.
8. 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.

9 Select Apply.

Figure 1: Example date and time setting



Changing system options

On the System Config Options page, you can:

- Set the system idle timeout.
- Set the authentication timeout.
- Select the language for the web-base manager.
- Modify the dead gateway detection settings.

To set the system idle timeout

1 Go to **System > Config > Options**.

2 For Idle Timeout, type a number in minutes.

3 Select Apply.

Idle Timeout controls the amount of inactive time that the web-based manager waits before requiring the administrator to log in again.

The default idle time out is 5 minutes. The maximum idle time out is 480 minutes (8 hours).

To set the Auth timeout

1 Go to **System > Config > Options**.

2 For Auth Timeout, type a number in minutes.

3 Select Apply.

Auth Timeout controls the amount of inactive time that the firewall waits before requiring users to authenticate again. For more information, see "Users and authentication" on page 171.

The default Auth Timeout is 15 minutes. The maximum Auth Timeout is 480 minutes (8 hours).

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.

You can choose English, Simplified Chinese, Japanese, Korean, or Traditional Chinese.

Note: When the web-based manager language is set to use Simplified Chinese, Japanese, Korean, or Traditional Chinese, you can change to English by selecting the English button on the upper right of the web-based manager.

Modifying 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 "Adding a ping server to an interface" on page 97.

To modify the dead gateway detection settings

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.

Adding and editing administrator accounts

When the FortiGate unit is initially 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 can connect to the FortiGate unit.

There are three administration account access levels:

admin	Has all permissions. Can view, add, edit, and delete administrator accounts. Can view and change the FortiGate configuration. The admin user is the only user who can go to the System Status page and manually update firmware, update the antivirus definitions, update the attack definitions, download or upload system settings, restore the FortiGate unit to factory defaults, restart the FortiGate unit, and shut down the FortiGate unit. There is only one admin user.
Read & Write	Can view and change the FortiGate configuration. Can view but cannot add, edit, or delete administrator accounts. Can change own administrator account password. Cannot make changes to system settings from the System Status page.
Read Only	Can view the FortiGate configuration.

Adding new administrator accounts

From the admin account, use the following procedure to add new administrator accounts and control their permission levels.

To add an administrator account

1. Go to **System > Config > Admin**.
2. Select New to add an administrator account.
3. Type a login name for the administrator account.

   The login name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Type and confirm a password for the administrator account.

   For improved security, the password should be at least 6 characters long. The password can contain any characters except spaces.
5. Optionally type a Trusted Host IP address and netmask for the location from which the administrator can log into the web-based manager.

   If you want the administrator to be able to access the FortiGate unit from any address, set the trusted host to 0.0.0.0 and the netmask to 0.0.0.0.

   To limit the administrator to only access the FortiGate unit from a specific network, set the trusted host to the address of the network and set the netmask to the netmask for the network. For example, to limit an administrator to accessing the FortiGate unit from your internal network, set the trusted host to the address of your internal network (for example, 192.168.1.0) and set the netmask to 255.255.255.0.
6. Set the Permission level for the administrator.
7. Select OK to add the administrator account.

Editing administrator accounts

The admin account user can change individual administrator account passwords, configure the IP addresses from which administrators can access the web-based manager, and change the administrator permission levels.

Administrator account users with Read & Write access can change their own administrator passwords.

To edit an administrator account

1. Go to **System > Config > Admin**.
2. To change an administrator account password, select Change Password  .
3. Type the Old Password.
4. Type and confirm a new password.

   For improved security, the password should be at least 6 characters long. The password can contain any characters except spaces. If you enter a password that is less than 6 characters long, the system displays a warning message but still accepts the password.
5. Select OK.
6. To edit the settings of an administrator account, select Edit  .
7. Optionally type a Trusted Host IP address and netmask for the location from which the administrator can log into the web-based manager.

   If you want the administrator to be able to access the FortiGate unit from any address, set the trusted host to 0.0.0.0 and the netmask to 255.255.255.255.

   To limit the administrator to only be able to access the FortiGate unit from a specific network, set the trusted host to the address of the network and set the netmask to the netmask for the network. For example, to limit an administrator to accessing the FortiGate unit from your internal network, set the trusted host to the address of your internal network (for example, 192.168.1.0) and set the netmask to 255.255.255.0.
8. Change the administrator's permission level as required.
9. Select OK.
10. To delete an administrator account, choose the account to delete and select Delete  .

Configuring SNMP

You can configure the FortiGate SNMP agent to report system information and send traps 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).

This section describes:

- Configuring the FortiGate unit for SNMP monitoring
- Configuring FortiGate SNMP support
- FortiGate MIBs
- FortiGate traps
- Fortinet MIB fields

Configuring the FortiGate unit for SNMP monitoring

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interfaces to accept SNMP connections. See “Controlling administrative access to an interface” on page 97.

Configuring FortiGate SNMP support

Use the information in this section to configure the FortiGate unit so that an SNMP manager can connect to the FortiGate SNMP agent to receive management information and traps.

- Configuring SNMP access to an interface
- Configuring SNMP community settings

Configuring SNMP access to an interface

Before a remote SNMP manager can connect to the FortiGate agent, you must configure one or more FortiGate interface‘s to accept SNMP connections. The configuration steps to follow depend on whether the FortiGate unit is operating in NAT/Route mode or Transparent mode.

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

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

To configure SNMP access to an interface in Transparent mode

1. Go to **System > Network > Management**.
2. Choose the interface that the SNMP manager connects to and select SNMP.

Select Apply.

Configuring SNMP community settings

You can configure a single SNMP community for each FortiGate device. An SNMP community consists of identifying information about the FortiGate unit, your SNMP get community and trap community strings, and the IP addresses of up to three SNMP managers that can receive traps sent by the FortiGate SNMP agent.

To configure SNMP community settings

1 Go to **System > Config > SNMP v1/v2c**.

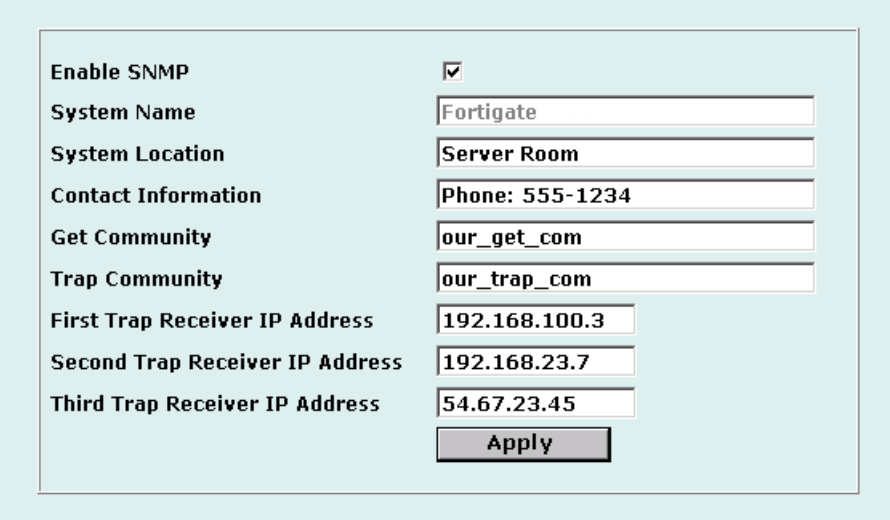
2 Select the Enable SNMP check box.

3 Configure the following SNMP settings:

System Name	Automatically set to the FortiGate host name. To change the System Name, see "Changing the FortiGate host name" on page 54.
System Location	Describe the physical location of the FortiGate unit. The system location description can be up to 31 characters long and can contain spaces, numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. The \ < > [ ] ` $ % & characters are not allowed.
Contact Information	Add the contact information for the person responsible for this FortiGate unit. The contact information can be up to 31 characters long and can contain spaces, numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. The \ < > [ ] ` $ % & characters are not allowed.
Get Community	Also called read community, get community is a password to identify SNMP get requests sent to the FortiGate unit. When an SNMP manager sends a get request to the FortiGate unit, it must include the correct get community string. The default get community string is "public". Change the default get community string to keep intruders from using get requests to retrieve information about your network configuration. The get community string must be used in your SNMP manager to enable it to access FortiGate SNMP information. The get community string can be up to 31 characters long and can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Spaces and the \ < > [ ] ` $ % & characters are not allowed.
Trap Community	The trap community string functions like a password that is sent with SNMP traps. The default trap community string is "public". Change the trap community string to the one accepted by your trap receivers. The trap community string can be up to 31 characters long and can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Spaces and the \ < > [ ] ` $ % & characters are not allowed.
Trap Receiver IP Addresses	Type the IP addresses of up to three trap receivers on your network that are configured to receive traps from your FortiGate unit. Traps are only sent to the configured addresses.

4 Select Apply.

Figure 2: Sample SNMP configuration



FortiGate MIBs

The FortiGate SNMP agent supports FortiGate proprietary MIBs as well as standard RFC 1213 and RFC 2665 MIBs. The FortiGate MIBs are listed in Table 1. 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 1: FortiGate MIBs

MIB file name or RFC	Description
fortinet-trap.mib	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 "FortiGate traps" on page 129.
fortinet.mib	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.
RFC-1213 (MIB II)	The FortiGate SNMP agent supports MIB II groups with the following exceptions.
	No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).
	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.
RFC-2665 (Ethernet-like MIB)	The FortiGate SNMP agent supports Ethernet-like MIB information with the following exception.
	No support for the dot3Tests and dot3Errors groups.

FortiGate traps

The FortiGate agent can send traps to up to three SNMP trap receivers on your network that are configured to receive traps from the FortiGate unit. For these SNMP managers to receive traps, you must load and compile the Fortinet trap MIB onto the SNMP manager.

General FortiGate traps

Table 2: General FortiGate traps

Trap message	Description
Cold Start	The FortiGate unit starts or restarts. An administrator enables the SNMP agent or changes FortiGate SNMP settings. This trap is sent when the agent starts during system startup.
System Down	The SNMP agent stops because the FortiGate unit shuts down.
Agent Down	An administrator disables the SNMP agent.
Agent Up	An administrator enables the SNMP agent. This trap is also sent when the agent starts during system startup.
The <interface_name> Interface IP is changed to <new_IP> (Serial No.: <FortiGate_serial_no>)	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.

System traps

Table 3: FortiGate system traps

Trap message	Description
interface <interface_name> is up.	An interface changes from the up state to the running state, indicating that the interface has been connected to a network. When the interface is up it is administratively up but not connected to a network. When the interface is running it is administratively up and connected to a network.
interface <interface_name> is down.	An interface changes from the running state to the up state, indicating that the interface has been disconnected from a network.
CPU usage high	CPU usage exceeds 90%.
memory low	Memory 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 switch	The primary unit in an HA cluster fails and is replaced with a new primary unit.

VPN traps

Table 4: FortiGate VPN traps

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

NIDS traps

Table 5: FortiGate NIDS traps

Trap message	Description
Flood attack happened.	NIDS attack prevention detects and provides protection from a syn flood attack.
Port scan attack happened.	NIDS attack prevention detects and provides protection from a port scan attack.

Antivirus traps

Table 6: FortiGate antivirus traps

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

Logging traps

Table 7: FortiGate logging traps

Trap message	Description
log full	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%.

Fortinet MIB fields

The Fortinet MIB contains fields for configuration settings and current status information for all parts of the FortiGate product. This section lists the names of the high-level MIB fields and describes the configuration and status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the fortinet.mib file into your SNMP manager and browsing the Fortinet MIB fields.

System configuration and status

Table 8: System MIB fields

MIB field	Description
fnSysStatus	FortiGate system configuration including operation mode, firmware version, virus definition version, attack definition version, and serial number. Status monitor information including current CPU usage, CPU idle status, CPU interrupts, memory usage, system up time, the number of active communication sessions, as well as descriptive information for each active communication session.
fnSysUpdate	FortiGate system update configuration including connection status to the FDN, push update status, periodic update status, and current virus and attack definitions versions.
fnSysNetwork	FortiGate system network configuration including the interface, VLAN, routing, DHCP, zone, and DNS configuration.
fnSysConfig	FortiGate system configuration including time, options, administrative users, and HA configuration.
fnSysSnmp	FortiGate SNMP configuration.

Firewall configuration

Table 9: Firewall MIB fields

MIB field	Description
fnFirewallPolicy	FortiGate firewall policy list including complete configuration information for each policy.
fnFirewallAddress	FortiGate firewall address and address group list.
fnFirewallService	FortiGate firewall service and service group list.
fnFirewallSchedule	FortiGate firewall schedule list.
fnFirewallVirtualIP	FortiGate firewall virtual IP list.
fnFirewallIpPool	FortiGate firewall IP pool list.
fnFirewallIPMACBinding	FortiGate firewall IP/MAC binding configuration.
fnFirewallContProfiles	FortiGate firewall content profile list.

Users and authentication configuration

Table 10: User and authentication MIB fields

FnUserLocalTable	Local user list.
FnUserRadiusSrvTable	RADIUS server list.
FnUserGrpTable	User group list.

VPN configuration and status

Table 11: VPN MIB fields

fnVpnIpsec	IPSec VPN configuration including the Phase 1 list, Phase 2 list, manual key list, and VPN concentrator list. Status and timeout for each VPN tunnel (Phase 2) and the dialup monitor list showing dialup tunnel status.
fnVpnPPTP	PPTP VPN configuration.
fnVpnL2TP	L2TP VPN configuration.
fnVpnCert	IPSec VPN with certificates configuration.

NIDS configuration

Table 12: NIDS MIB fields

fnNidsDetection	NIDS detection configuration.
fnNidsPrevention	NIDS prevention configuration.
fnNidsResponse	NIDS response configuration.

Antivirus configuration

Table 13: Antivirus MIB fields

fnAvFileBlock	Antivirus file blocking configuration.
fnAvQuarantine	Antivirus quarantine configuration.
fnAVConfig	Antivirus configuration including the current virus definition virus list.

Web filter configuration

Table 14: Web filter MIB fields

fnWebFiltercfgMsgTable	Web filter content block list and configuration.
fnWebFilterUrlBlk	Web filter URL block list.
fnWebFilterScripts	Web filter script blocking configuration.
fnWebFilterExemptUrl	Web filter exempt URL list.

Logging and reporting configuration

Table 15: Logging and reporting MIB fields

fnLoglogSetting	Log setting configuration.
fnLoglog	Log setting traffic filter configuration.
fnLogAlertEmail	Alert email configuration.

Replacement messages

Replacement messages are added to content passing through the firewall to replace:

- Files or other content removed from POP3 and IMAP email messages by the antivirus system,
- Files or other content removed from HTTP downloads by the antivirus system or web filtering,
- Files removed from FTP downloads by the antivirus system.

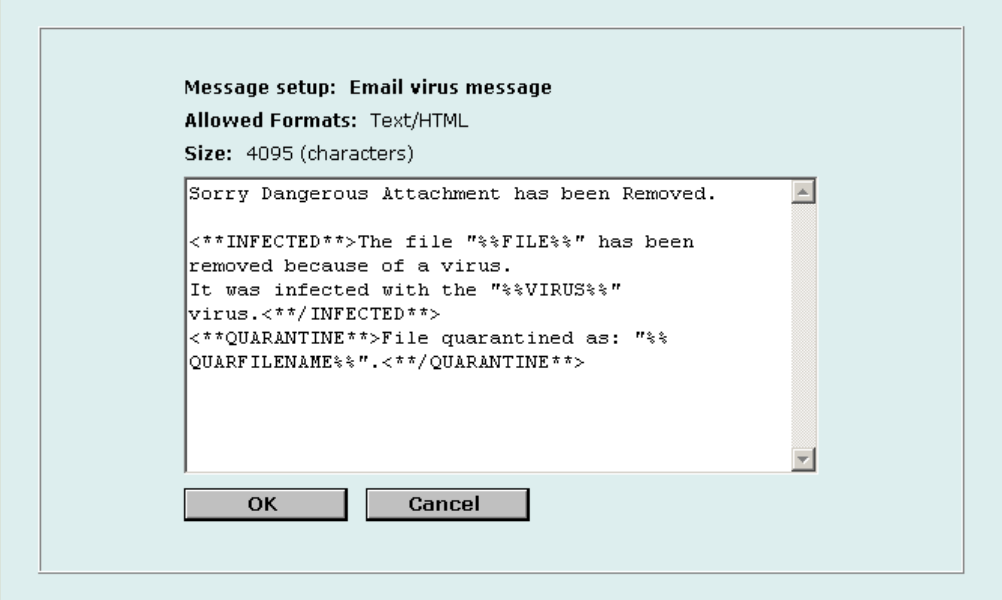
You can edit the content of replacement messages.

You can also edit the content added to alert email messages to control the information that appears in alert emails for virus incidents, NIDS events, critical system events, and disk full events.

This section describes:

- Customizing replacement messages
- Customizing alert emails

Figure 3: Sample replacement message



Customizing replacement messages

Each of the replacement messages in the replacement message list is created by combining replacement message sections. You can use these sections as building blocks to create your own replacement messages.

You can edit any of the replacement messages in the replacement message list and add and edit the replacement message sections as required.

To customize a replacement message

1 Go to **System > Config > Replacement Messages**.

2 For the replacement message that you want to customize, select Modify  .

3 In the Message setup dialog box, edit the content of the message.
Table 16 lists the replacement message sections that can be added to replacement messages and describes the tags that can appear in each section. In addition to the allowed tags you can add text. For mail and HTTP messages you can also add HTML code.

4 Select OK to save the changes.

Table 16: Replacement message sections

File blocking	Used for file blocking (all services).	
Section Start	<**BLOCKED**>	
Allowed Tags	%%FILE%%	The name of the file that was blocked.
	%%URL%%	The URL of the blocked web page.
Section End	<**/BLOCKED**>	

Scanning	Used for virus scanning (all services).	
Section Start	<**INFECTED**>	
Allowed Tags	%%FILE%%	The name of the file that was infected.
	%%VIRUS%%	The name of the virus infecting the file.
	%%URL%%	The URL of the blocked web page or file.
Section End	<**/INFECTED**>	

Quarantine	Used when quarantine is enabled (permitted for all scan services and block services for email only).	
Section Start	<**QUARANTINE**>	
Allowed Tag	%%QUARFILE NAME%%	The name of the file that was quarantined.
Section End	<**/QUARANTINE**>	

Customizing alert emails

Customize alert emails to control the content displayed in alert email messages sent to system administrators.

To customize alert emails

1 Go to **System > Config > Replacement Messages**.

2 For the alert email message that you want to customize, select Modify  .

3 In the Message setup dialog box, edit the text of the message.
Table 17 lists the replacement message sections that can be added to alert email messages and describes the tags that can appear in each section. In addition to the allowed tags you can add text and HTML code.

4 Select OK to save the changes.

Table 17: Alert email message sections

NIDS event	Used for NIDS event alert email messages	
Section Start	<**NIDS_EVENT**>	
Allowed Tags	%%NIDS_EVENT%%	The NIDS attack message.
Section End	<**/NIDS_EVENT**>	

Virus alert	Used for virus alert email messages	
Section Start	<**VIRUS_ALERT**>	
Allowed Tags	%%VIRUS%%	The name of the virus.
	%%PROTOCOL%%	The service for which the virus was detected.
	%%SOURCE_IP%%	The IP address from which the 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.
	%%DEST_IP%%	The IP address of the computer that would have received the virus. For POP3 this is the IP address of the user's computer that attempted to download the email containing the virus.
	%%EMAIL_FROM%%	The email address of the sender of the message in which the virus was found.
	%%EMAIL_TO%%	The email address of the intended receiver of the message in which the virus was found.
Section End	<**/VIRUS_ALERT**>	

Block alert	Used for file block alert email messages	
Section Start	<**BLOCK_ALERT**>	
Allowed Tags	%%FILE%%	The name of the file that was blocked.
	%%PROTOCOL%%	The service for which the file was blocked.
	%%SOURCE_IP%%	The IP address from which the block file was received. For email this is the IP address of the email server that sent the email containing the blocked file. For HTTP this is the IP address of web page that sent the blocked file.
	%%DEST_IP%%	The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file ware removed.
	%%EMAIL_FROM%%	The email address of the sender of the message from which the file was removed.
	%%EMAIL_TO%%	The email address of the intended receiver of the message from which the file was removed.
Section End	<**/BLOCK_ALERT**>	

Critical event	Used for critical firewall event alert emails.	
Section Start	<**CRITICAL_EVENT**>	
Allowed Tags	%%CRITICAL_EVENT%%	The firewall critical event message
Section End	<**/CRITICAL_EVENT**>	

Firewall configuration

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 (port number).

For the packet to be connected through the FortiGate unit, a firewall policy must be in place that matches the source address, destination address, and service of the packet. 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. You can also add schedules to policies so that the firewall can process connections differently depending on the time of day or the day of the week, month, or year.

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 content profiles to policies to apply antivirus protection, web filtering, and email filtering to web, file transfer, and email services. You can create content profiles that perform one or any combination of the following actions:

- Apply antivirus protection to HTTP, FTP, SMTP, IMAP, or POP3 services.
- Apply web filtering to HTTP services.
- Apply email filtering to IMAP and POP3 services.

You can also add logging to a firewall policy so that the FortiGate unit logs all connections that use this policy.

This chapter describes:

Default firewall configuration

Firewall policies control connections between interfaces. By default, the users on your internal network can connect through the FortiGate unit to the Internet. The firewall blocks all other connections.

The firewall is configured with a default policy that matches any connection request received from the internal network and instructs the firewall to forward the connection to the Internet.

The default policy also applies virus scanning to all HTTP, FTP, SMTP, POP3, and IMAP traffic matched by the policy. The policy applies virus scanning because the Antivirus & Web Filter option is selected and the Content profile is set to Scan. For more information about content profiles, see “Content profiles” on page 166.

Figure 4: Default firewall policy

#	ID	Source	Dest	Schedule	Service	Action	Enable	Config
1	1	Internal_All	External_All	Always	ANY	ACCEPT	☑	

- Addresses
- Services
- Schedules
- Content profiles

Addresses

Add policies to control connections between FortiGate interfaces and between the networks connected to these interfaces. To add policies between interfaces, the interfaces must include addresses. By default the FortiGate unit is configured with two firewall addresses:

- Internal_All, added to the internal interface, this address matches all addresses on the internal network.
- External_All, added to the external interface, this address matches all addresses on the external network.

The firewall uses these addresses to match the source and destination addresses of packets received by the firewall. The default policy matches all connections from the internal network because it includes the Internal_All address. The default policy also matches all connections to the external network because it includes the External_All address.

You can add more addresses to each interface to improve the control you have over connections through the firewall. For more information about firewall addresses, see "Addresses" on page 146.

You can also add firewall policies that perform network address translation (NAT). To use NAT to translate destination addresses, you must add virtual IPs. Virtual IPs map addresses on one network to a translated address on another network. For more information about Virtual IPs, see "Virtual IPs" on page 157.

Services

Policies can control connections based on the service or destination port number of packets. The default policy accepts connections using any service or destination port number. The firewall is configured with over 40 predefined services. You can add these services to a policy for more control over the services that can be used by connections through the firewall. You can also add user-defined services. For more information about services, see "Services" on page 149.

Schedules

Policies can control connections based on the time of day or day of the week when the firewall receives the connection. The default policy accepts connections at any time. The firewall is configured with one schedule that accepts connections at any time. You can add more schedules to control when policies are active. For more information about schedules, see "Schedules" on page 154.

Content profiles

Add content profiles to policies to apply antivirus protection, web filtering, and email filtering to web, file transfer, and email services. The FortiGate unit includes the following default content profiles:

- Strict—to apply maximum content protection to HTTP, FTP, IMAP, POP3, and SMTP content traffic.
- Scan—to apply antivirus scanning to HTTP, FTP, IMAP, POP3, and SMTP content traffic.
- Web—to apply antivirus scanning and Web content blocking to HTTP content traffic.
- Unfiltered—to allow oversized files to pass through the FortiGate unit without scanned for viruses.

The default policy includes the scan content profile.

For more information about content profiles, see "Content profiles" on page 166.

Adding firewall policies

Add Firewall policies to control connections and traffic between FortiGate interfaces.

To add a firewall policy

1. Go to **Firewall > Policy**.
2. Select the policy list to which you want to add the policy.
3. Select New to add a new policy.
   You can also select Insert Policy before  on a policy in the list to add the new policy above a specific policy.
4. Configure the policy:
   For information about configuring the policy, see "Firewall policy options" on page 140.
5. Select OK to add the policy.
6. 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 "Configuring policy lists" on page 144.

Firewall policy options

This section describes the options that you can add to firewall policies.

Source

Select an address or address group that matches the source address of the packet. Before you can add this address to a policy, you must add it to the source interface. For information about adding an address, see "Addresses" on page 146.

Destination

Select an address or address group that matches the destination address of the packet. Before you can add this address to a policy, you must add it to the destination interface. For information about adding an address, see "Addresses" on page 146.

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 "Virtual IPs" on page 157.

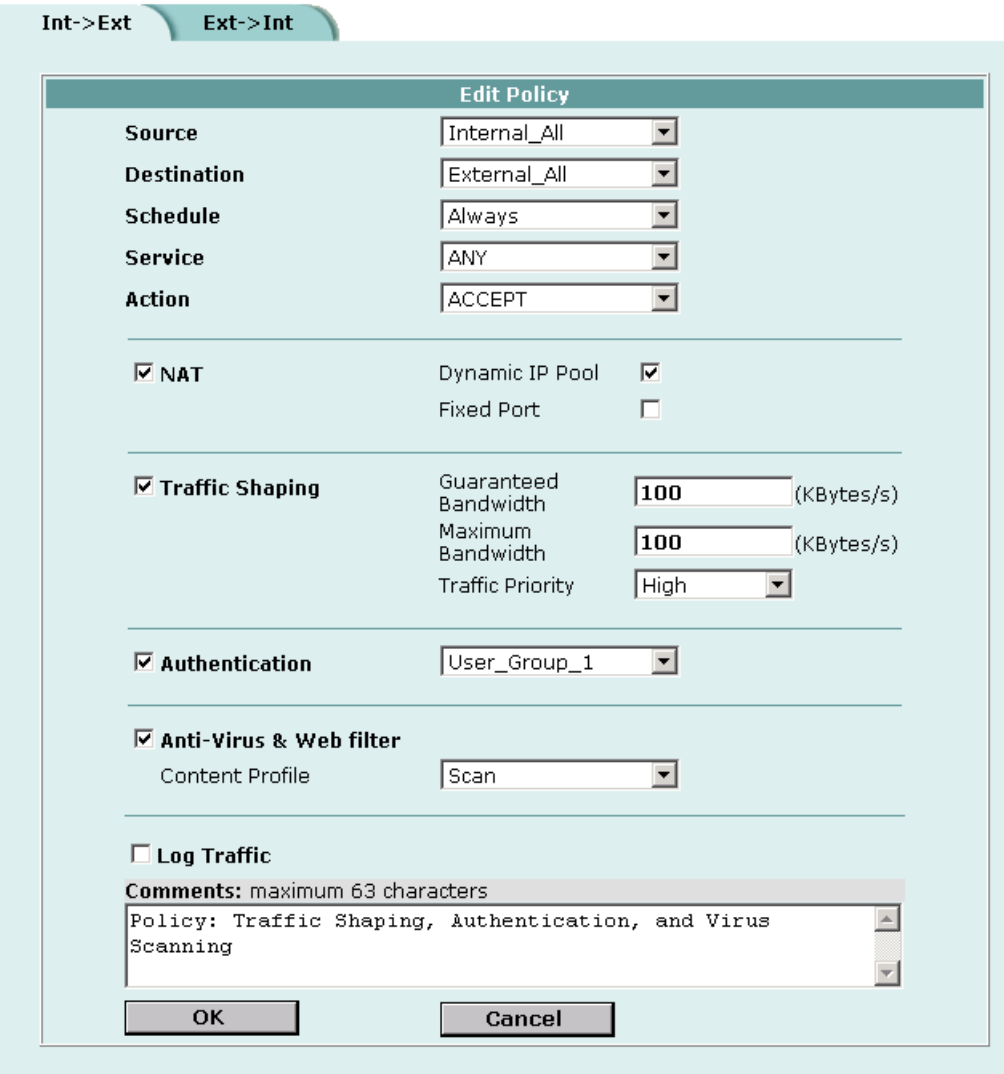
Schedule

Select a schedule that controls when the policy is available to be matched with connections. See "Schedules" on page 154.

Service

Select a service that matches the service (port number) of the packet. You can select from a wide range of predefined services or add custom services and service groups. See "Services" on page 149.

Figure 5: Adding a NAT/Route policy



Action

Select how you want the firewall to respond when the policy matches a connection attempt.

ACCEPT	Accept the connection. If you select ACCEPT, you can also configure NAT and Authentication for the policy.
DENY	Deny the connection. The only other policy option that you can configure is Log Traffic, to log the connections denied by this policy.
ENCRYPT	Make this policy an IPSec VPN policy. If you select ENCRYPT, 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. ENCRYPT is not available in Transparent mode. See "Configuring encrypt policies" on page 193.

NAT

Configure the policy for NAT. NAT translates the source address and the source 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.

Dynamic IP Pool Select Dynamic IP Pool to translate the source address to an address randomly selected from an IP pool. The IP pool must be added to the destination interface of the policy.
You cannot select Dynamic IP Pool if the destination interface is configured using DHCP or PPPoE.
For information about adding IP pools, see "IP pools" on page 161.

Fixed Port 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.

VPN Tunnel

Select a VPN tunnel for an ENCRYPT policy. You can select an AutoIKE key or Manual Key tunnel. VPN Tunnel is not available in Transparent mode.

Allow inbound Select Allow inbound so that users behind the remote VPN gateway can connect to the source address.

Allow outbound Select Allow outbound so that users can connect to the destination address behind the remote VPN gateway.

Inbound NAT Select Inbound NAT to translate the source address of incoming packets to the FortiGate internal IP address.

Outbound NAT Select Outbound NAT to translate the source address of outgoing packets to the FortiGate external IP address.

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 the policy does not allow any traffic.

Guaranteed Bandwidth 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.

Maximum Bandwidth	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.
Traffic Priority	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.

Authentication

Select Authentication and select a user group to require users to enter a user name and password before the firewall accepts the connection. Select the user group to control the users that can authenticate with this policy. For information about adding and configuring user groups, see “Configuring user groups” on page 177. You must add user groups before you can select 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.

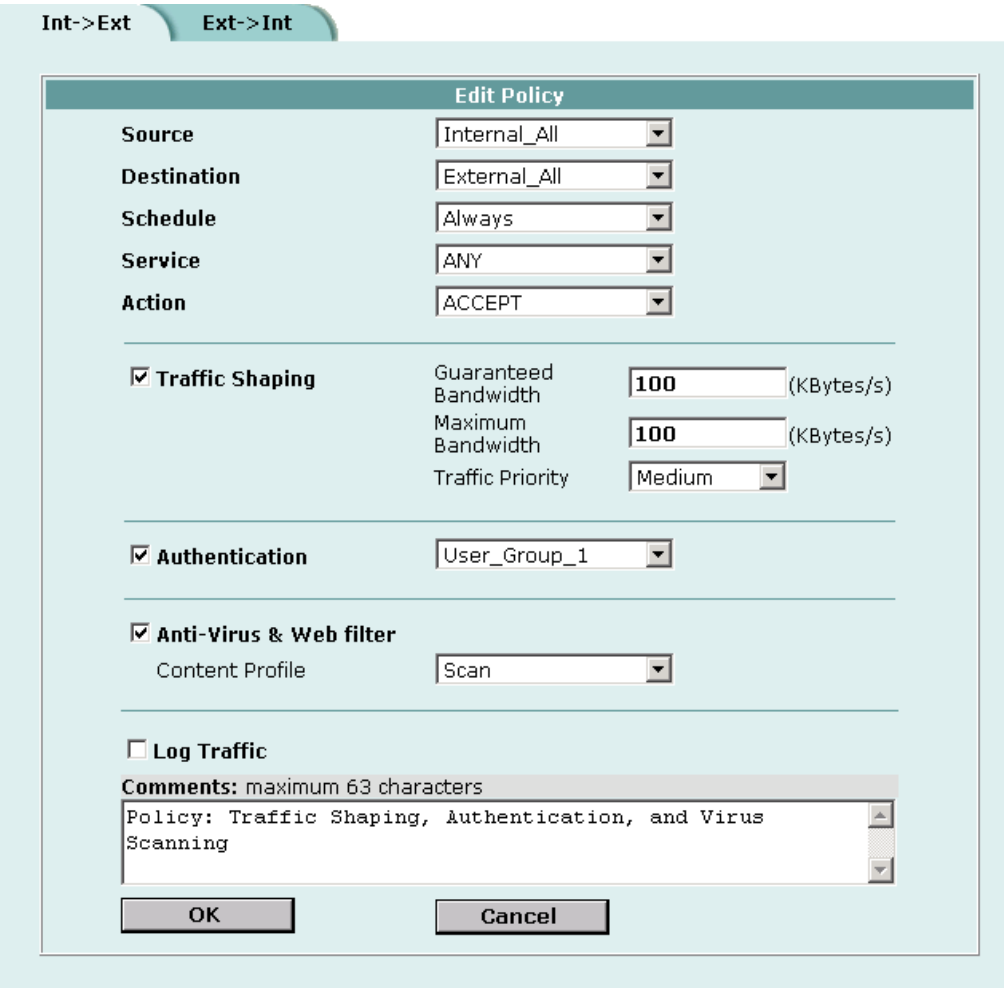
In most cases you should make sure that users can use DNS through the firewall without authentication. If DNS is not available users cannot connect to a web, FTP, or Telnet server using a domain name.

Anti-Virus & Web filter

Enable antivirus protection and web filter content filtering for traffic controlled by this policy. You can select Anti-Virus & Web filter if Service is set to ANY, HTTP, SMTP, POP3, IMAP, or FTP or to a service group that includes the HTTP, SMTP, POP3, IMAP, or FTP services.

Select a content profile to configure how antivirus protection and content filtering is applied to the policy. For information about selecting a content profile, see “Content profiles” on page 166.

Figure 6: Adding a Transparent mode policy



Log Traffic

Select Log Traffic to write messages to the traffic log whenever the policy processes a connection. For information about logging, see "Logging and reporting" on page 251.

Comments

You can add a description or other information about the policy. The comment can be up to 63 characters long, including spaces.

Configuring policy lists

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:

- Policy matching in detail
- Changing the order of policies in a policy list
- Enabling and disabling policies

Policy matching in detail

When the FortiGate unit receives a connection attempt at an interface, it must select 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.

The default policy accepts all connection attempts from the internal network to the Internet. From the internal network, users can browse the web, use POP3 to get email, use FTP to download files through the firewall, and so on. If the default policy is at the top of the Int->Ext policy list, the firewall allows all connections from the internal network to the Internet because all connections match the default policy. If more specific policies are added to the list below the default policy, they are never matched.

A policy that is an exception to the default policy, for example, a policy to block FTP connections, must be placed above the default policy in the Int->Ext policy list. In this example, all FTP connection attempts from the internal network would then match the FTP policy and be blocked. Connection attempts for all other kinds of services would not match with the FTP policy but they would match with the default policy. Therefore, the firewall would still accept all other connections from the internal network.

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.

Changing the order of policies in a policy list

To change the order of a policy in a policy list

1. Go to **Firewall > Policy**.
2. Select the policy list that you want to change the order of.
3. Choose the policy that you want to move and select Move To  to change its order in the policy list.
4. Type a number in the Move to field to specify where in the policy list to move the policy and select OK.

Enabling and disabling policies

You can enable and disable policies in the policy list to control whether the policy is active or not. The FortiGate unit matches enabled policies but does not match disabled policies.

Disabling policies

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. For information about stopping active communication sessions, see "System status" on page 67.

To disable a policy

1. Go to **Firewall > Policy**.
2. Select the policy list that contains the policy that you want to disable.
3. Clear the check box of the policy to disable it.

Enabling policies

Enable a policy that has been disabled so that the firewall can match connections with the policy.

To enable a policy

1. Go to **Firewall > Policy**.
2. Select the policy list that contains the policy that you want to enable.
3. Select the check box of the policy to enable it.

Addresses

All policies require source and destination addresses. To add addresses to a policy between two interfaces, you must first add addresses to the address list for each interface.

You can add, edit, and delete all firewall addresses as required. You can also organize related addresses into address groups to simplify policy creation.

A firewall address consists of an IP address and a netmask. This information 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)

Note: IP address: 0.0.0.0 and Netmask: 255.255.255.255 is not a valid firewall address.

This section describes:

- Adding addresses
- Editing addresses
- Deleting addresses
- Organizing addresses into address groups

Adding addresses

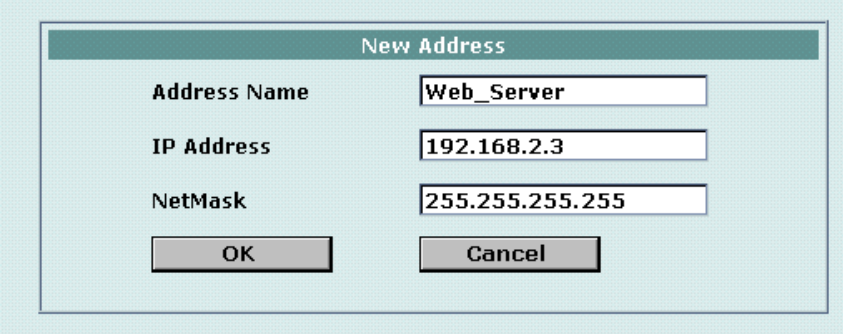
To add an address

1. Go to **Firewall > Address**.
2. Select the interface that you want to add the address to.
3. Select New to add a new address.
4. Enter an Address Name to identify the address.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Spaces and other special characters are not allowed.
5. Enter the IP Address.
   The 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
6. Enter the Netmask.
   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

Note: To add an address to represent any address on a network set the IP Address to 0.0.0.0 and the Netmask to 0.0.0.0

7. Select OK to add the address.

Figure 7: Adding an internal address



Editing addresses

Edit an address to change its IP address and netmask. You cannot edit the address name. To change the address name, you must delete the address entry and then add the address again with a new name.

To edit an address

1. Go to **Firewall > Address**.
2. Select the interface list containing the address that you want to edit.
3. Choose an address to edit and select Edit Address  .
4. Make the required changes and select OK to save the changes.

Deleting addresses

Deleting an address removes it from an address list. To delete an address that has been added to a policy, you must first remove the address from the policy.

To delete an address

1. Go to **Firewall > Address**.
2. Select the interface list containing the address that you want to delete.
   You can delete any address that has a Delete Address icon  .
3. Choose an address to delete and select Delete  .
4. Select OK to delete the address.

Organizing addresses into address groups

You can organize related addresses into address groups to make it easier to add policies. For example, if you add three addresses and then add them to an address group, you only have to add one policy using the address group rather than a separate policy for each address.

You can add address groups to any interface. The address group can only contain addresses from that interface. Address groups are available in interface source or destination address lists.

Address groups cannot have the same names as individual addresses. If an address group is included in a policy, it cannot be deleted unless it is first removed from the policy.

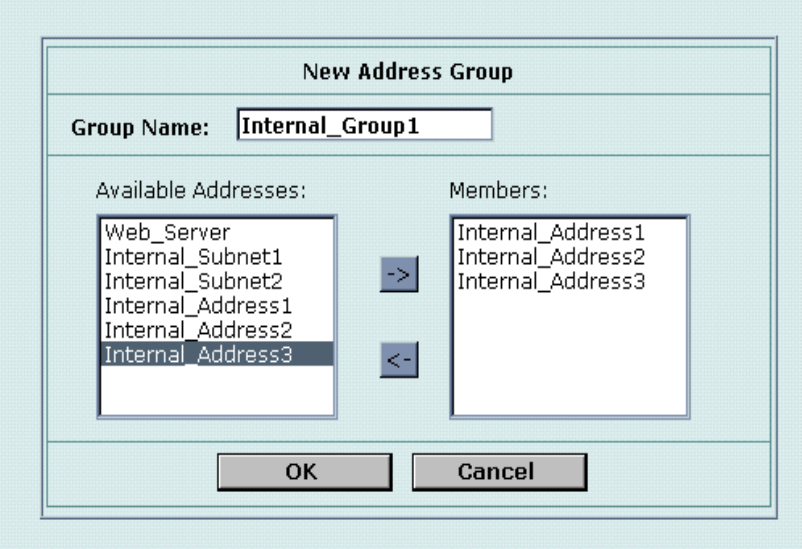
To organize addresses into an address group

1. Go to **Firewall > Address > Group**.
2. Select the interface that you want to add the address group to.
3. Enter a Group Name to identify the address group.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. To add addresses to the address group, select an address from the Available Addresses list and select the right arrow to add it to the Members list.

5 To remove addresses from the address group, select an address from the Members list and select the left arrow to remove it from the group.

6 Select OK to add the address group.

Figure 8: Adding an internal address group



Services

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 services
- Adding custom TCP and UDP services
- Adding custom ICMP services
- Adding custom IP services
- Grouping services

Predefined services

The FortiGate predefined firewall services are listed in Table 18. You can add these services to any policy.

Table 18: 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

Table 18: FortiGate predefined services (Continued)

Service name	Description	Protocol	Port
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-Relay	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
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

Table 18: FortiGate predefined services (Continued)

Service name	Description	Protocol	Port
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
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 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
SMTP	For sending 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	SSH 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

Table 18: FortiGate predefined services (Continued)

Service name	Description	Protocol	Port
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, 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. 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

Adding custom TCP and UDP services

Add a custom TCP or UDP service if you need to create a policy for a service that is not in the predefined service list.

To add a custom TCP or UDP service

1. Go to **Firewall > Service > Custom**.
2. Select TCP/UDP from the Protocol list.
3. Select New.
4. Type a Name for the new custom TCP or UDP service. This name appears in the service list used when you add a policy.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
5. Select the Protocol (either TCP or UDP) used by the service.
6. Specify a Source and 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.
7. If the service has more than one port range, select Add to specify additional protocols and port ranges.
   If there are too many port range rows, select Delete to remove each extra row.
8. Select OK to add the custom service.
   You can now add this custom service to a policy.

Adding custom ICMP services

Add a custom ICMP service if you need to create a policy for a service that is not in the predefined service list.

To add a custom ICMP service

1. Go to **Firewall > Service > Custom**.
2. Select ICMP from the Protocol list.
3. Select New.
4. Type a Name for the new custom ICMP service. This name appears in the service list used when you add a policy.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
5. Specify the ICMP type and code for the service.
6. Select OK to add the custom service.
   You can now add this custom service to a policy.

Adding custom IP services

Add a custom IP service if you need to create a policy for a service that is not in the predefined service list.

To add a custom IP service

1. Go to **Firewall > Service > Custom**.
2. Select IP from the Protocol list.
3. Select New.
4. Type a Name for the new custom IP service. This name appears in the service list used when you add a policy.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
5. Specify the IP protocol number for the service.
6. Select OK to add the custom service.
   You can now add this custom service to a policy.

Grouping services

To make it easier to add policies, you can create groups of services and then add one policy to provide or block access for all the services in the group. A service group can contain predefined services and custom services in any combination. You cannot add service groups to another service group.

To group services

1. Go to **Firewall > Service > Group**.
2. Select New.

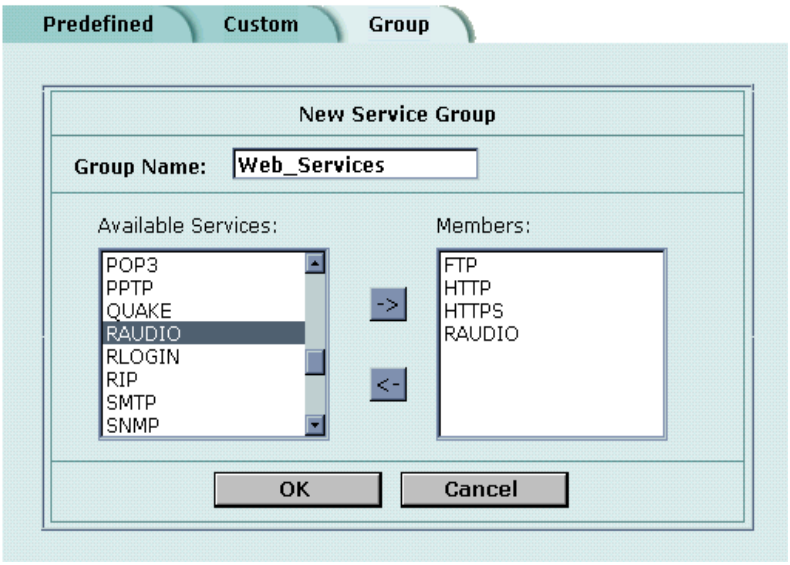
3 Type a Group Name to identify the group.
This name appears in the service list when you add a policy and cannot be the same as a predefined service name.
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

4 To add services to the service group, select a service from the Available Services list and select the right arrow to copy it to the Members list.

5 To remove services from the service group, select a service from the Members list and select the left arrow to remove it from the group.

6 Select OK to add the service group.

Figure 9: Adding a service group



Schedules

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:

- Creating one-time schedules
- Creating recurring schedules
- Adding schedules to policies

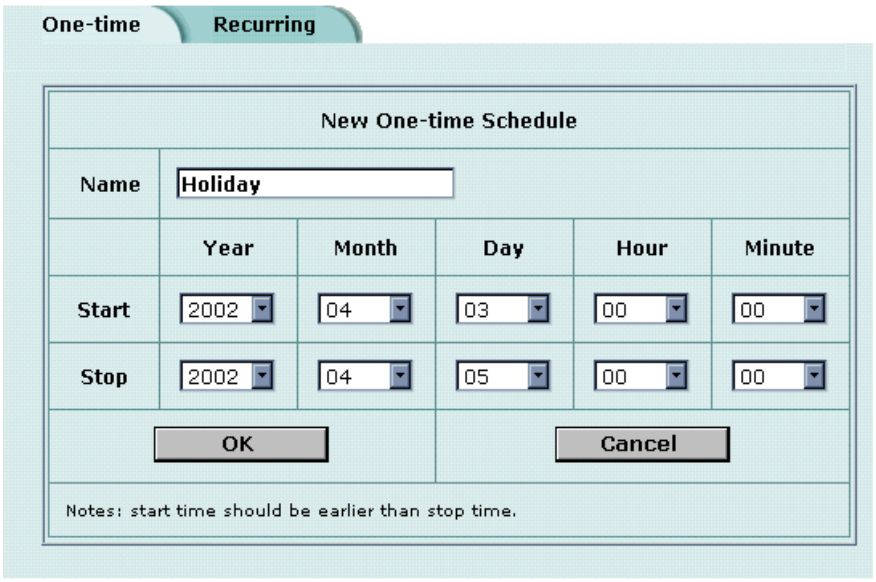
Creating one-time schedules

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.

To create a one-time schedule

1. Go to **Firewall > Schedule > One-time**.
2. Select New.
3. Type a Name for the schedule.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Set the Start date and time for the schedule.
   Set Start and Stop times to 00 for the schedule to be active for the entire day.
5. Set the Stop date and time for the schedule.
   One-time schedules use a 24-hour clock.
6. Select OK to add the one-time schedule.

Figure 10: Adding a one-time schedule



Creating recurring schedules

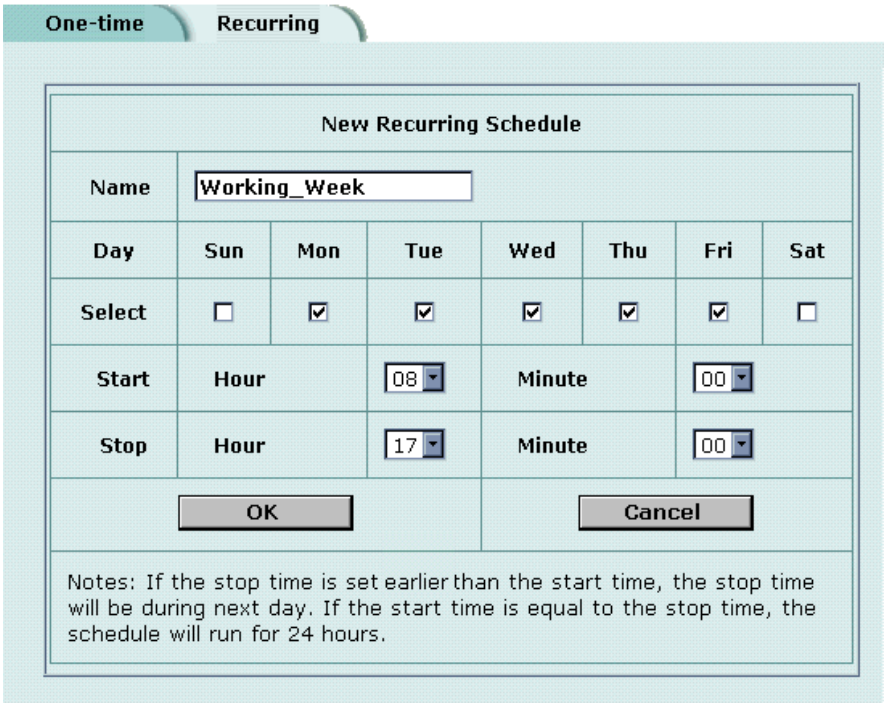
You can create a recurring schedule that activates or deactivates policies at specified times of the day or on specified days of the week. For example, you might want to prevent Internet use outside working hours by creating a recurring schedule.

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.

To create a recurring schedule

1. Go to **Firewall > Schedule > Recurring**.
2. Select New to create a new schedule.
3. Type a Name for the schedule.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Select the days of the week that you want the schedule to be active on.
5. Set the Start and Stop hours in between which you want the schedule to be active.
   Recurring schedules use a 24-hour clock.
6. Select OK to save the recurring schedule.

Figure 11: Adding a recurring schedule



Adding schedules to policies

After you create schedules, you can add them to policies to schedule when the policies are active. You can add the new schedules to policies when you create the policy, or you can edit existing policies and add a new schedule to them.

To add a schedule to a policy

1. Go to **Firewall > Policy**.
2. Create a new policy or edit a policy to change its schedule.
3. Configure the policy as required.
4. Add a schedule by selecting it from the Schedule list.
5. Select OK to save the policy.
6. Arrange the policy in the policy list to have the effect that you expect.

   For example, to use a one-time schedule to deny access to a policy, add a policy that matches the policy to be denied in every way. Choose the one-time schedule that you added and set Action to DENY. Then place the policy containing the one-time schedule in the policy list above the policy to be denied.

Virtual IPs

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 internal network, it might have a private IP address such as 192.168.1.34. 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 internal network. To allow connections from the Internet to the web server, you must then add an Ext->Int firewall policy and set Destination to the virtual IP.

You can create two 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.

This section describes:

- Adding static NAT virtual IPs
- Adding port forwarding virtual IPs
- Adding policies with virtual IPs

Adding static NAT virtual IPs

To add a static NAT virtual IP

1 Go to **Firewall > Virtual IP**.

2 Select New to add a virtual IP.

3 Type a Name for the virtual IP.

The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

4 Select the virtual IP External Interface from the list.

The external interface is the interface connected to the source network that receives the packets to be forwarded to the destination network.

You can set the virtual IP external interface to any FortiGate interface. Table 19 contains example virtual IP external interface settings and describes the policies that you can add the resulting virtual IP to.

Table 19: Virtual IP External Interface examples

External Interface	Description
internal	To map an internal address to an external address. If you select internal, the static NAT virtual IP can be added to Int->Ext policies.
external	To map an external address to an internal address. If you select external, the static NAT virtual IP can be added to Ext->Int policies.

5 In the Type section, 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, this address must be routed to this interface. The virtual IP address and the external IP address can be on different subnets.

If the IP address of the external interface selected in step 4 is set using PPPoE or DHCP, you can enter 0.0.0.0 for the external IP address. The FortiGate unit substitutes the IP address set for this external interface using PPPoE or DHCP.

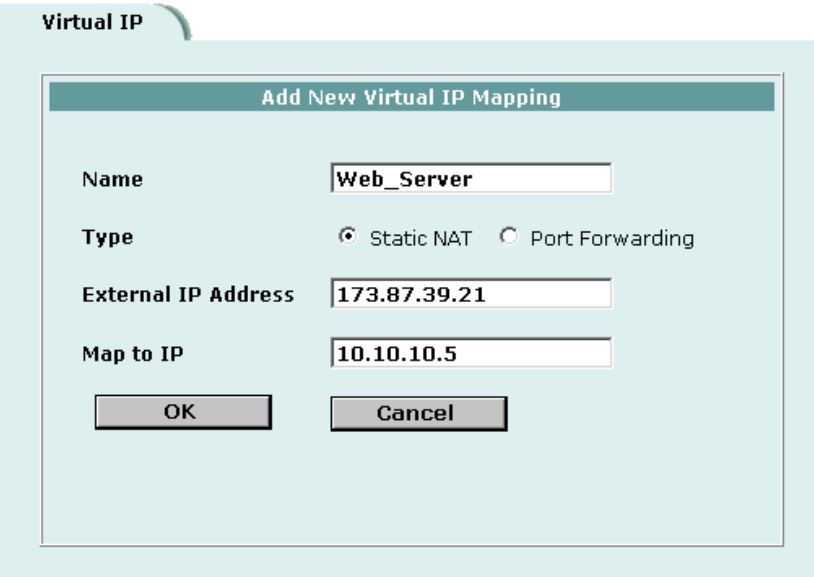
7 In Map to IP, type the real IP address on the destination network, for example, the IP address of a web server on an internal network.

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 to save the virtual IP.

You can now add the virtual IP to firewall policies.

Figure 12: Adding a static NAT virtual IP



Adding port forwarding virtual IPs

To add port forwarding virtual IPs

1. Go to **Firewall > Virtual IP**.
2. Select New to add a virtual IP.
3. Type a Name for the virtual IP.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Select the virtual IP External Interface from the list.
   The external interface is the interface connected to the source network that receives the packets to be forwarded to the destination network.
5. In the Type section, select Port Forwarding.
6. Enter the External IP Address that you want to map to an address on the destination zone.
   You can set the external IP address to the IP address of the external interface selected in step 4 or to any other address.
   If the IP address of the external interface selected in step 4 is set using PPPoE or DHCP, you can enter 0.0.0.0 for the External IP Address. The FortiGate unit substitutes the IP address set for this external interface using PPPoE or DHCP.
   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 that you want to configure port forwarding for.

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 In Map to IP, enter the real IP address on the destination network.

For example, the real IP address could be the IP address of a web server on an internal network.

9 In Map to Port, enter the port number to be added to packets when they are forwarded.

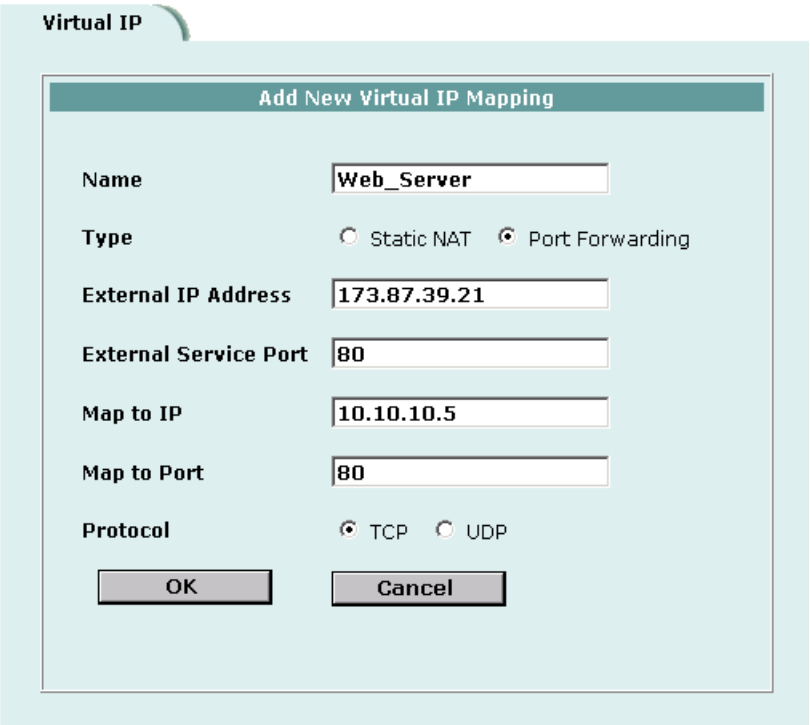
If you do not want to translate the port, enter the same number as the External Service Port.

If you want to translate the port, enter the port number to which to translate the destination port of the packets when they are forwarded by the firewall.

10 Select the protocol (TCP or UDP) that you want the forwarded packets to use.

11 Select OK to save the port forwarding virtual IP.

Figure 13: Adding a port forwarding virtual IP



Adding policies with virtual IPs

Use the following procedure to add a policy that uses a virtual IP to forward packets.

To add a policy with a virtual IP

1 Go to **Firewall > Policy**.

2 Select the type of policy that you want to add.

- The source interface must match the interface selected in the External Interface list.
- The destination interface must match the interface connected to the network with the Map to IP address.

3 Use the following information to configure the policy.

Source	Select the source address from which users can access the server.
Destination	Select the virtual IP.
Schedule	Select a schedule as required.
Service	Select the service that matches the Map to Service that you selected for the port-forwarding virtual IP.
Action	Set action to ACCEPT to accept connections to the internal server. You can also select DENY to deny access.
NAT	Select NAT if the firewall is protecting the private addresses on the destination network from the source network.
Authentication	Optionally select Authentication and select a user group to require users to authenticate with the firewall before accessing the server using port forwarding.
Log Traffic **Anti-Virus & Web filter**	Select these options to log port-forwarded traffic and apply antivirus and web filter protection to this traffic.

4 Select OK to save the policy.

IP pools

An IP pool (also called a dynamic IP pool) is a range of IP addresses added to a firewall interface. If you add IP pools to an interface, you can select Dynamic IP Pool when you configure a policy with the destination set to this 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.

For example, if you add an IP pool to the internal interface, you can select Dynamic IP pool for Ext->Int policies.

You can add multiple IP pools to any interface but only the first IP pool is used by the firewall.

This section describes:

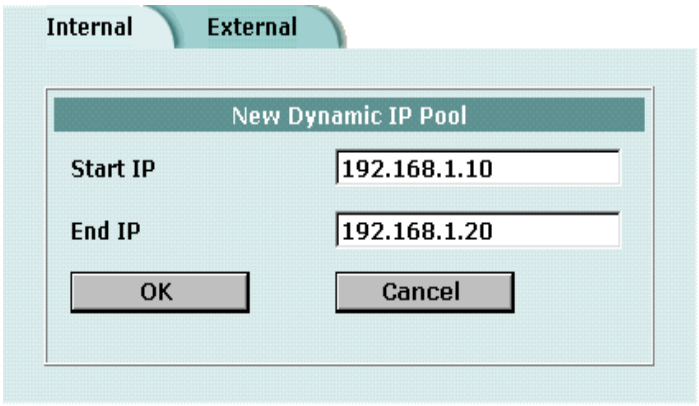
- Adding an IP pool
- IP Pools for firewall policies that use fixed ports
- IP pools and dynamic NAT

Adding an IP pool

To add an IP pool

1. Go to **Firewall > IP Pool**.
2. Select the interface to which to add the IP pool.
3. Select New to add a new IP pool to the selected interface.
4. Enter the Start IP and End IP addresses for the range of addresses in the IP pool. The start IP and end IP must define the start and end of an address range. The start IP must be lower than the end IP. The start IP and end IP must be on the same subnet as the IP address of the interface that you are adding the IP pool.
5. Select OK to save the IP pool.

Figure 14: Adding an IP Pool



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.

IP/MAC binding

IP/MAC binding protects the FortiGate unit and your network from IP spoofing attacks. IP spoofing attacks try to use the IP address of a trusted computer to connect to, or through, the FortiGate unit from a different computer. The IP address of a computer is easy to change to a trusted address, but MAC addresses are added to ethernet cards at the factory and are not easy to change.

You can enter the static IP addresses and corresponding MAC addresses of trusted computers in the static IP/MAC table.

If you have trusted computers with dynamic IP addresses that are set by the FortiGate DHCP server, the FortiGate unit adds these IP addresses and their corresponding MAC addresses to the dynamic IP/MAC table. For information about viewing the table, see "Viewing a DHCP server dynamic IP list" on page 107. The dynamic IP/MAC binding table is not available in Transparent mode.

You can enable IP/MAC binding for packets in sessions connecting to the firewall or passing through the firewall.

Note: If you enable IP/MAC binding and change the IP address of a computer with an IP or MAC address in the IP/MAC list, you must also change the entry in the IP/MAC list or the computer does not have access to or through the FortiGate unit. You must also add the IP/MAC address pair of any new computer that you add to your network or the new computer does not have access to or through the FortiGate unit.

This section describes:

- Configuring IP/MAC binding for packets going through the firewall
- Configuring IP/MAC binding for packets going to the firewall
- Adding IP/MAC addresses
- Viewing the dynamic IP/MAC list
- Enabling IP/MAC binding

Configuring IP/MAC binding for packets going through the firewall

Use the following procedure to use IP/MAC binding to filter packets that a firewall policy would normally allow through the firewall.

To configure IP/MAC binding for packets going through the firewall

1. Go to **Firewall > IP/MAC Binding > Setting**.
2. Select the Enable IP/MAC binding going through the firewall check box.
3. Go to **Firewall > IP/MAC Binding > Static IP/MAC**.

4 Select New to add IP/MAC binding pairs to the IP/MAC binding list.

All packets that would normally be allowed through the firewall by a firewall policy are first compared with the entries in the IP/MAC binding list. If a match is found, then the firewall attempts to match the packet with a policy.

For example, if the IP/MAC pair IP 1.1.1.1 and 12:34:56:78:90:ab:cd is added to the IP/MAC binding list:

- A packet with IP address 1.1.1.1 and MAC address 12:34:56:78:90:ab:cd is allowed to go on to be matched with a firewall policy.
- A packet with IP 1.1.1.1 but with a different MAC address is dropped immediately to prevent IP spoofing.
- A packet with a different IP address but with a MAC address of 12:34:56:78:90:ab:cd is dropped immediately to prevent IP spoofing.
- A packet with both the IP address and MAC address not defined in the IP/MAC binding table:
  - is allowed to go on to be matched with a firewall policy if IP/MAC binding is set to Allow traffic,
  - is blocked if IP/MAC binding is set to Block traffic.

Configuring IP/MAC binding for packets going to the firewall

Use the following procedure to use IP/MAC binding to filter packets that would normally connect with the firewall (for example, when an administrator is connecting to the FortiGate unit for management).

To configure IP/MAC binding for packets going to the firewall

1 Go to **Firewall > IP/MAC Binding > Setting**.

2 Select the Enable IP/MAC binding going to the firewall check box.

3 Go to **Firewall > IP/MAC Binding > Static IP/MAC**.

4 Select New to add IP/MAC binding pairs to the IP/MAC binding list.

All packets that would normally connect to the firewall are first compared with the entries in the IP/MAC binding table.

For example, if the IP/MAC pair IP 1.1.1.1 and 12:34:56:78:90:ab:cd is added to the IP/MAC binding list:

- A packet with IP address 1.1.1.1 and MAC address 12:34:56:78:90:ab:cd is allowed to connect to the firewall.
- A packet with IP 1.1.1.1 but with a different MAC address is dropped immediately to prevent IP spoofing.
- A packet with a different IP address but with a MAC address of 12:34:56:78:90:ab:cd is dropped immediately to prevent IP spoofing.
- A packet with both the IP address and MAC address not defined in the IP/MAC binding table:
  - is allowed to connect to the firewall if IP/MAC binding is set to Allow traffic,
  - is blocked if IP/MAC binding is set to Block traffic.

Adding IP/MAC addresses

To add an IP/MAC address

1. Go to **Firewall > IP/MAC Binding > Static IP/MAC**.
2. Select New to add an IP address/MAC address pair.
3. Enter the IP Address and the MAC Address.
   You can bind multiple IP addresses to the same MAC address. You cannot bind multiple MAC addresses to the same IP address.
   However, you can set the IP address to 0.0.0.0 for multiple MAC addresses. This means that all packets with these MAC addresses are matched with the IP/MAC binding list.
   Similarly, you can set the MAC address to 00:00:00:00:00:00 for multiple IP addresses. This means that all packets with these IP addresses are matched with the IP/MAC binding list.
4. Type a Name for the new IP/MAC address pair.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
5. Select the Enable check box to enable IP/MAC binding for the IP/MAC pair.
6. Select OK to save the IP/MAC binding pair.

Viewing the dynamic IP/MAC list

To view the dynamic IP/MAC list

1. Go to **Firewall > IP/MAC Binding > Dynamic IP/MAC**.

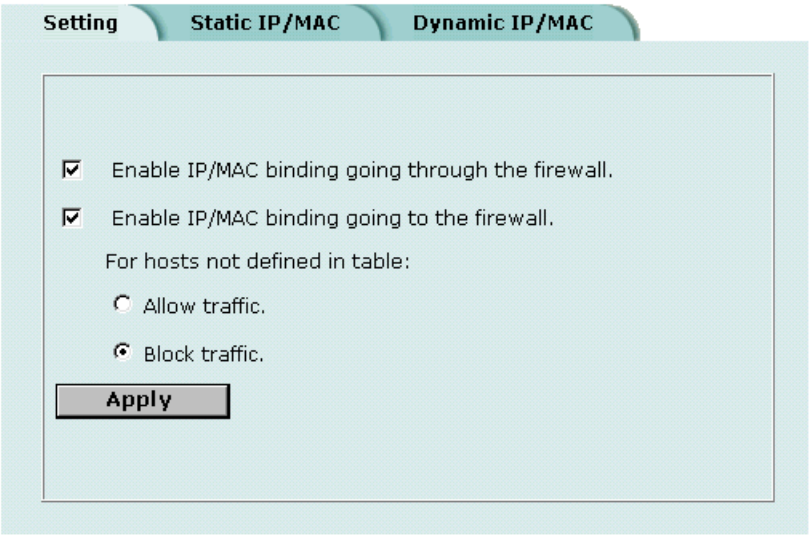
Enabling IP/MAC binding

Caution: Make sure that you have added the IP/MAC Address pair of your management computer before enabling IP/MAC binding.

To enable IP/MAC binding

1. Go to **Firewall > IP/MAC Binding > Setting**.
2. Select the Enable IP/MAC binding going through the firewall check box if you want to turn on IP/MAC binding for packets that could be matched by policies.
3. Select the Enable IP/MAC binding going to the firewall check box if you want to turn on IP/MAC binding for packets connecting to the firewall.
4. Configure how IP/MAC binding handles packets with IP and MAC addresses that are not defined in the IP/MAC list.
   Select Allow traffic to allow all packets with IP and MAC address pairs that are not added to the IP/MAC binding list.
   Select Block traffic to block packets with IP and MAC address pairs that are not added to the IP/MAC binding list.
5. Select Apply to save the changes.

Figure 15: IP/MAC settings



Content profiles

Use content profiles to apply different protection settings for content traffic that is controlled by firewall policies. You can use content profiles to:

- Configure antivirus protection for HTTP, FTP, POP3, SMTP, and IMAP policies
- Configure web filtering for HTTP policies
- Configure email filtering for IMAP and POP3 policies
- Configure oversized file and email blocking for HTTP, FTP, POP3, SMTP, and IMAP policies
- Pass fragmented email for POP3, SMTP, and IMAP policies

Using content profiles, you can build protection configurations that can be applied to different types of firewall policies. This allows you to 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 content profiles.

Content profiles can be added to NAT/Route mode and Transparent mode policies.

- Default content profiles
- Adding content profiles
- Adding content profiles to policies

Default content profiles

The FortiGate unit has the following four default content profiles that are displayed on the Firewall Content Profile page. You can use the default content profiles or create your own.

Strict	To apply maximum content protection to HTTP, FTP, IMAP, POP3, and SMTP content traffic. You would not use the strict content profile under normal circumstances but it is available if you have extreme problems with viruses and require maximum content screening protection.
Scan	To apply antivirus scanning to HTTP, FTP, IMAP, POP3, and SMTP content traffic.
Web	To apply antivirus scanning and web content blocking to HTTP content traffic. You can add this content profile to firewall policies that control HTTP traffic.
Unfiltered	Use if you do not want to apply content protection to content traffic. You can add this content profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected.

Adding content profiles

If the default content profiles do not provide the protection that you require, you can create custom content profiles.

To add a content profile

1 Go to **Firewall > Content Profile**.

2 Select New.

3 Type a Profile Name.

4 Enable the antivirus protection options that you want.

Anti Virus Scan	Scan web, FTP, and email traffic for viruses and worms. See "Antivirus scanning" on page 226.
File Block	Delete files with blocked file patterns even if they do not contain viruses. Enable file blocking when a virus has been found that is so new that virus scanning does not detect it. See "File blocking" on page 227.

Note: If both Anti Virus Scan and File Block are enabled, the FortiGate unit blocks files that match enabled file patterns before they are scanned for viruses.

5 Enable the web filtering options that you want.

Web URL Block	Block unwanted web pages and web sites. This option adds FortiGate Web URL blocking (see "Configuring FortiGate Web URL blocking" on page 235), FortiGate Web Pattern blocking (see "Configuring FortiGate Web pattern blocking" on page 237), and Cerberian URL filtering (see "Configuring Cerberian URL filtering" on page 238) to HTTP traffic accepted by a policy.
Web Content Block	Block web pages that contain unwanted words or phrases. See "Content blocking" on page 232.
Web Script Filter	Remove scripts from web pages. See "Script filtering" on page 240.

Web Exempt List Exempt URLs from web filtering and virus scanning. See "Exempt URL list" on page 241.

6 Enable the email filter protection options that you want.

Email Block List Add a subject tag to email from unwanted addresses. See "Email block list" on page 248.

Email Exempt List Exempt sender address patterns from email filtering. See "Email exempt list" on page 249.

Email Content Block Add a subject tag to email that contains unwanted words or phrases. See "Email banned word list" on page 246.

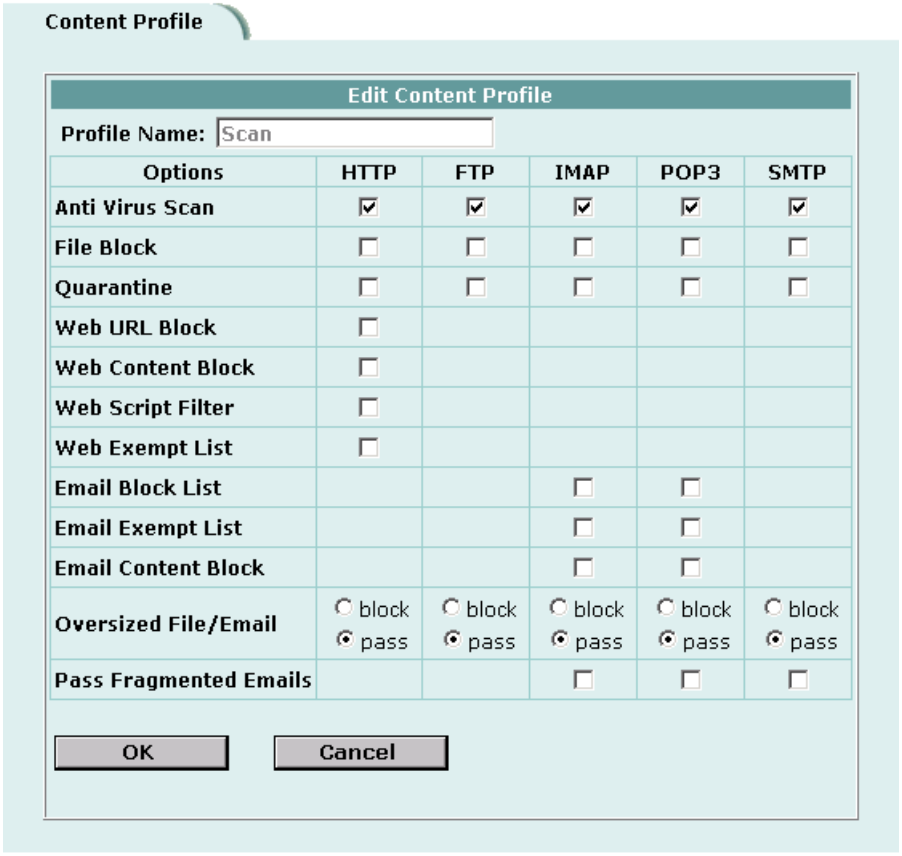
7 Enable the fragmented email and oversized file and email options that you want.

Oversized File/Email Block or pass files and email that exceed thresholds configured as a percent of system memory. See "Blocking oversized files and emails" on page 228.

Pass Fragmented Email Allow email messages that have been fragmented to bypass antivirus scanning. See "Exempting fragmented email from blocking" on page 228.

8 Select OK.

Figure 16: Example content profile



Adding content profiles to policies

You can add content profiles to 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.

To add a content profile to a policy

1. Go to **Firewall > Policy**.
2. Select a policy list that contains policies that you want to add a content profile to.
   For example, to enable network protection for files downloaded by internal network users from the web, select an internal to external policy list.
3. Select New to add a new policy, or choose a policy and select Edit  .
4. Select the Anti-Virus & Web filter check box.
5. Select a content profile from the list.
6. Configure the remaining policy settings, if required.
7. Select OK.
8. Repeat this procedure for any policies that you want to enable network protection for.

Users and authentication

FortiGate units support user authentication to the FortiGate user database, a RADIUS server, and an LDAP server. You can add user names to the FortiGate user database and then add a password to allow the user to authenticate using the internal database. You can also add the names of RADIUS and LDAP servers. You can select RADIUS to allow the user to authenticate using the selected RADIUS server or LDAP to allow the user to authenticate using the selected LDAP server. You can disable a user name so that the user cannot authenticate.

To enable authentication, you must add user names to one or more user groups. You can also add RADIUS servers and LDAP servers to user groups. You can then select a user group when you require authentication.

You can select user groups to require authentication for:

- any firewall policy with Action set to ACCEPT
- IPSec dialup user phase 1 configurations
- XAuth functionality for phase 1 IPSec VPN configurations
- PPTP
- L2TP

When a user enters a user name and password, the FortiGate unit searches the internal user database for a matching user name. If Disable is selected for that user name, the user cannot authenticate and the connection is dropped. If Password is selected for that user and the password matches, the connection is allowed. If the password does not match, the connection is dropped.

If RADIUS is selected and RADIUS support is configured and the user name and password match a user name and password on the RADIUS server, the connection is allowed. If the user name and password do not match a user name and password on the RADIUS server, the connection is dropped.

If LDAP is selected and LDAP support is configured and the user name and password match a user name and password on the LDAP server, the connection is allowed. If the user name and password do not match a user name and password on the LDAP server, the connection is dropped.

If the user group contains user names, RADIUS servers, and LDAP servers, the FortiGate unit checks them in the order in which they have been added to the user group.

This chapter describes:

Setting authentication timeout

Authentication timeout controls how long authenticated firewall connections can remain idle before users must authenticate again to get access through the firewall.

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.

Adding user names and configuring authentication

Use the following procedures to add user names and configure authentication.

This section describes:

Adding user names and configuring authentication

To add a user name and configure authentication

1 Go to **User > Local**.

2 Select New to add a new user name.

3 Type the User Name.
The user name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

4 Select one of the following authentication configurations:

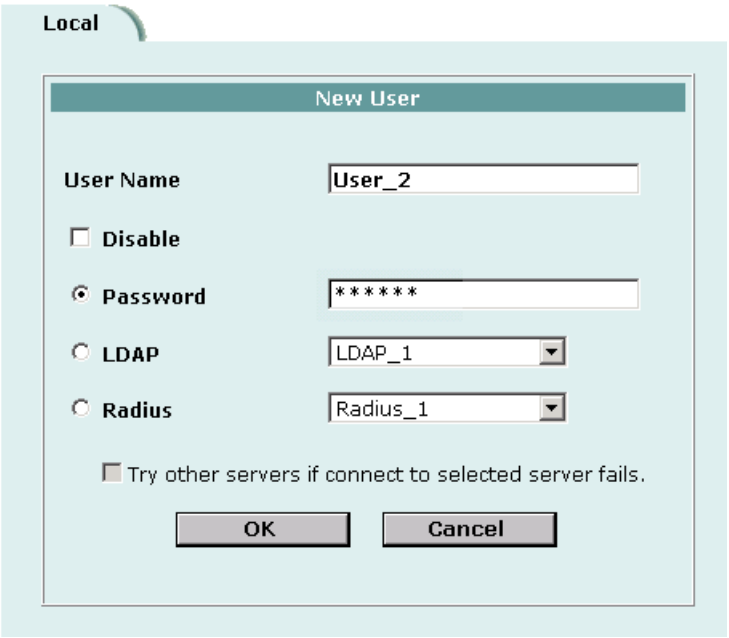
Disable	Prevent this user from authenticating.
Password	Enter the password that this user must use to authenticate. The password should be at least six characters long. The password can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

LDAP	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 "Configuring LDAP support" on page 175.
Radius	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 "Configuring RADIUS support" on page 174.

5 Select the Try other servers if connect to selected server fails check box if you have selected Radius and you want the FortiGate unit to try to connect to other RADIUS servers added to the FortiGate RADIUS configuration.

6 Select OK.

Figure 17: Adding a user name



Deleting user names 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.

To delete a user name from the internal database

1 Go to **User > Local**.

2 Select Delete User for the user name that you want to delete.

3 Select OK.

Note: Deleting the user name deletes the authentication configured for the user.

Configuring RADIUS support

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.

This section describes:

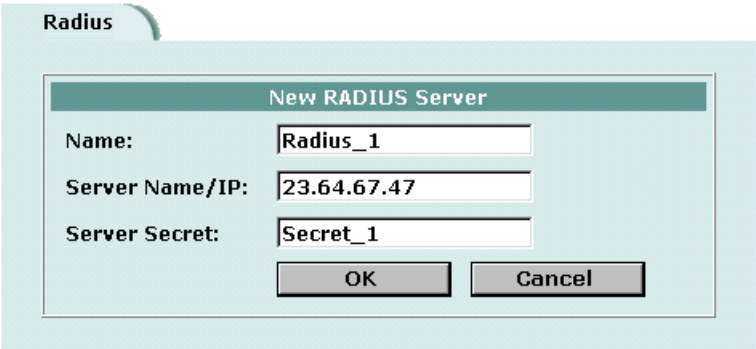
- Adding RADIUS servers
- Deleting RADIUS servers

Adding RADIUS servers

To add a RADIUS server

1. Go to **User > RADIUS**.
2. Select New to add a new RADIUS server.
3. Type the Name of the RADIUS server.
   You can type any name. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Enter the Server Name or IP address of the RADIUS server.
5. Enter the RADIUS server secret.
6. Select OK.

Figure 18: Example RADIUS configuration



Deleting RADIUS servers

You cannot delete a RADIUS server that has been added to a user group.

To delete a RADIUS server

1. Go to **User > RADIUS**.
2. Select Delete beside the RADIUS server name that you want to delete.
3. Select OK.

Configuring LDAP support

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. ForitGate LDAP supports all LDAP servers compliant with LDAP v3.

FortiGate LDAP support does not extend to proprietary functionality, such as notification of password expiration, that is available from some LDAP servers. FortiGate LDAP support does not supply information to the user about why authentication failed.

LDAP user authentication is supported for PPTP, L2TP, IPSec VPN, and firewall authentication. With PPTP, L2TP, and IPSec VPN, PAP (packet authentication protocol) is supported and CHAP (Challenge-Handshake Authentication Protocol) is not.

This section describes:

Adding LDAP servers

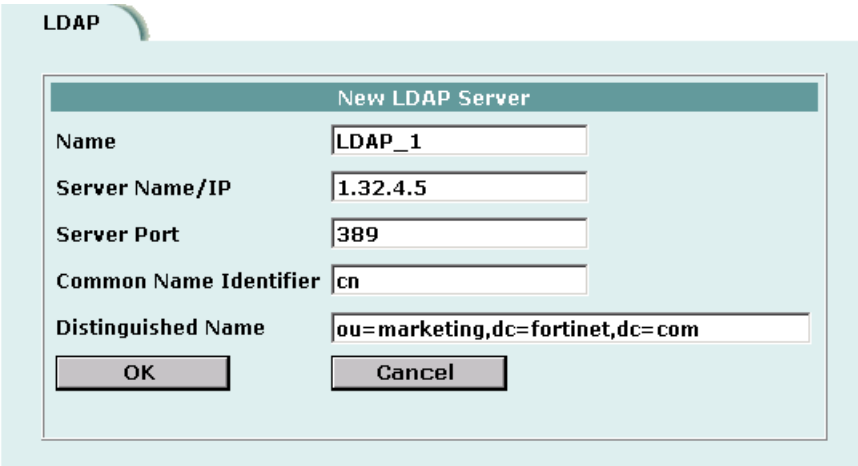
To add an LDAP server

1. Go to **User > LDAP**.
2. Select New to add a new LDAP server.
3. Type the Name of the LDAP server.
   You can type any name. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Enter the Server Name or IP address of the LDAP server.
5. Enter the Server Port used to communicate with the LDAP server.
   By default LDAP uses port 389.
6. 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.

7 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

8 Select OK.

Figure 19: Example LDAP configuration



Deleting LDAP servers

You cannot delete an LDAP server that has been added to a user group.

To delete an LDAP server

1 Go to **User > LDAP**.

2 Select Delete beside the LDAP server name that you want to delete.

3 Select OK.

Configuring user groups

To enable authentication, you must add user names, RADIUS servers, and LDAP servers to one or more user groups. You can then select a user group when you require authentication. You can select a user group to configure authentication for:

- Policies that require authentication. Only users in the selected user group or users that can authenticate with the RADIUS servers added to the user group can 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 users 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.

If the user group contains users, RADIUS servers, and LDAP servers, the FortiGate unit checks them in the order in which they have been added to the user group.

This section describes:

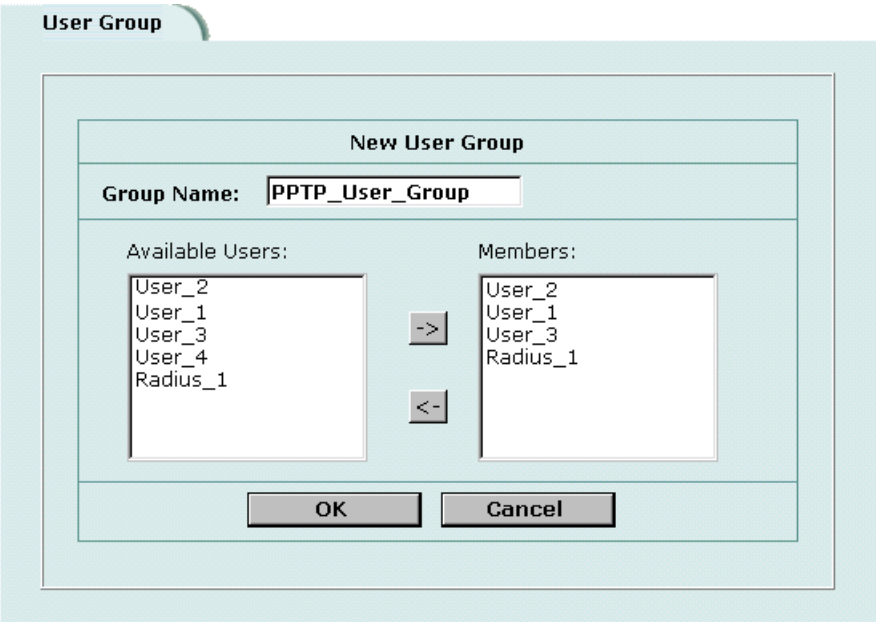
Adding user groups

Use the following procedure to add user groups to the FortiGate configuration. You can add user names, RADIUS servers, and LDAP servers to user groups.

To add a user group

1. Go to **User > User Group**.
2. Select New to add a new user group.
3. Enter a Group Name to identify the user group.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
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.

Figure 20: Adding a user group



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 OK.

Deleting user groups

You cannot delete user groups that have been selected in a policy, a dialup user phase 1 configuration, or a PPTP or L2TP configuration.

To delete a user group

1 Go to **User > User Group**

2 Select Delete beside the user group that you want to delete.

3 Select OK.

IPSec VPN

A Virtual Private Network (VPN) is an extension of a private network that encompasses links across shared or public networks such as the Internet. For example, a company that has two offices in different cities, each with its own private network, can use a VPN to create a secure tunnel between the offices. Similarly, a teleworker can use a VPN client for remote access to a private office network. In both cases, the secure connection appears to the user as a private network communication, even though the communication is over a public network.

Secure VPN connections are enabled by a combination of tunneling, data encryption, and authentication. Tunneling encapsulates data so that it can be transferred over the public network. Instead of being sent in its original format, the data frames are encapsulated within an additional header and then routed between tunnel endpoints. Upon arrival at the destination endpoint, the data is decapsulated and forwarded to its destination within the private network.

Encryption changes a data stream from clear text (something that a human or a program can interpret) to cipher text (something that cannot be interpreted). The information is encrypted and decrypted using mathematical algorithms known as keys.

Authentication provides a means to verify the origin of a packet and the integrity of its contents. Authentication is done using checksums calculated with keyed hash function algorithms.

This chapter provides an overview about how to configure FortiGate IPSec VPN. For a complete description of FortiGate VPN, see the *FortiGate VPN Guide*.

Key management

There are three basic elements in any encryption system:

- an algorithm that changes information into code,
- a cryptographic key that serves as a secret starting point for the algorithm,
- a management system to control the key.

IPSec provides two ways to handle key exchange and management:

- Manual Keys
- Automatic Internet Key Exchange (AutoIKE) with pre-shared keys or certificates

Manual Keys

When using manual keys, matching security settings must be entered at both ends of the tunnel. These settings, which include both the encryption and authentication keys, must be kept secret so that unauthorized parties cannot decrypt the data, even if they know which encryption algorithm is being used.

Automatic Internet Key Exchange (AutoIKE) with pre-shared keys or certificates

For using multiple tunnels, an automated system of key management is required. IPSec supports the automated generation and negotiation of keys using the Internet Key Exchange protocol. This method of key management is referred to as AutoIKE. Fortinet supports AutoIKE with pre-shared keys and AutoIKE with certificates.

AutoIKE with pre-shared keys

If both peers in a session are configured with the same pre-shared key, they can use it to authenticate themselves to each other. The peers do not send the key to each other. Instead, as part of the security negotiation process, they use it in combination with a Diffie-Hellman group to create a session key. The session key is used for encryption and authentication and is automatically regenerated by IKE during the communication session.

Pre-shared keys are similar to manual keys in that they require the network administrator to distribute and manage matching information at the VPN peer sites. Whenever a pre-shared key changes, the administrator must update both sites.

AutoIKE with certificates

This method of key management involves a trusted third party, the certificate authority (CA). Each peer in a VPN is first required to generate a set of keys, known as a public/private key pair. The CA signs the public key for each peer, creating a signed digital certificate. The peer then contacts the CA to retrieve their own certificates, plus that of the CA. After the certificates are uploaded to the FortiGate units and appropriate IPSec tunnels and policies are configured, the peers are ready to communicate. As they do, IKE manages the exchange of certificates, sending signed digital certificates from one peer to another. The signed digital certificates are validated by the presence of the CA certificate at each end. With authentication complete, the IPSec tunnel is then established.

In some respects, certificates are simpler to manage than manual keys or pre-shared keys. For this reason, certificates are best suited to large network deployments.

Manual key IPSec VPNs

When using manual keys, complementary security parameters must be entered at both ends of the tunnel. In addition to encryption and authentication algorithms and keys, the security parameter index (SPI) is required. The SPI is an arbitrary value that defines the structure of the communication between the peers. With other methods, the SPI is generated automatically but with the manual key configuration it must be entered as part of the VPN setup.

The encryption and authentication keys must match on the local and remote peers, that is, the SPI values must be mirror images of each other. After you enter these values, the VPN tunnel can start without a need for the authentication and encryption algorithms to be negotiated. Provided you entered correct, complementary values, the tunnels are established between the peers. This means that the tunnel already exists between the peers. As a result, when traffic matches a policy requiring the tunnel, it can be authenticated and encrypted immediately.

General configuration steps for a manual key VPN

A manual key VPN configuration consists of a manual key VPN tunnel, the source and destination addresses for both ends of the tunnel, and an encrypt policy to control access to the VPN tunnel.

To create a manual key VPN configuration

1. Add a manual key VPN tunnel. See “Adding a manual key VPN tunnel” on page 181.
2. Configure an encrypt policy that includes the tunnel, source address, and destination address for both ends of the tunnel. See “Configuring encrypt policies” on page 193.

Adding a manual key VPN tunnel

Configure a manual key tunnel to create an IPSec VPN tunnel between the FortiGate unit and a remote IPSec VPN client or gateway that is also using manual key.

To add a manual key VPN tunnel

1. Go to **VPN > IPSec > Manual Key**.
2. Select New to add a new manual key VPN tunnel.
3. Type a VPN Tunnel Name.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Enter the Local SPI.
   The Local Security Parameter Index is a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f) in the range bb8 to FFFFFFF. This number must be added to the Remote SPI at the opposite end of the tunnel.
5. Enter the Remote SPI.
   The Remote Security Parameter Index is a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f) in the range bb8 to FFFFFFF. This number must be added to the Local SPI at the opposite end of the tunnel.

6 Enter the Remote Gateway.
This is the external IP address of the FortiGate unit or other IPSec gateway at the opposite end of the tunnel.

7 Select an Encryption Algorithm from the list.
Use the same algorithm at both ends of the tunnel.

8 Enter the Encryption Key.
Each two-character combination entered in hexadecimal format represents one byte. Depending on the encryption algorithm that you select, you might be required to enter the key in multiple segments. Use the same encryption key at both ends of the tunnel.

DES	Enter a 16-character (8 byte) hexadecimal number (0-9, A-F).
3DES	Enter a 48-character (24 byte) hexadecimal number (0-9, A-F). Separate the number into three segments of 16 characters.
AES128	Enter a 32-character (16 byte) hexadecimal number (0-9, A-F). Separate the number into two segments of 16 characters.
AES192	Enter a 48-character (24 byte) hexadecimal number (0-9, A-F). Separate the number into three segments of 16 characters.
AES256	Enter a 64-character (32 byte) hexadecimal number (0-9, A-F). Separate the number into four segments of 16 characters.

9 Select an Authentication Algorithm from the list.
Use the same algorithm at both ends of the tunnel.

10 Enter the Authentication Key.
Each two-character combination entered in hexadecimal format represents one byte. Use the same authentication key at both ends of the tunnel.

MD5	Enter a 32-character (16 byte) hexadecimal number (0-9, A-F). Separate the number into two segments of 16 characters.
SHA1	Enter a 40-character (20 byte) hexadecimal number (0-9, A-F). Separate the number into two segments—the first of 16 characters; the second of 24 characters.

11 Select a concentrator if you want the tunnel to be part of a hub and spoke VPN configuration. See “Adding a VPN concentrator” on page 198.

12 Select OK to save the manual key VPN tunnel.

AutoIKE IPSec VPNs

FortiGate units support two methods of Automatic Internet Key Exchange (AutoIKE) for establishing IPSec VPN tunnels: AutoIKE with pre-shared keys and AutoIKE with digital certificates.

- General configuration steps for an AutoIKE VPN
- Adding a phase 1 configuration for an AutoIKE VPN
- Adding a phase 2 configuration for an AutoIKE VPN

General configuration steps for an AutoIKE VPN

An AutoIKE VPN configuration consists of phase 1 and phase 2 configuration parameters, the source and destination addresses for both ends of the tunnel, and an encrypt policy to control access to the VPN tunnel.

To create an AutoIKE VPN configuration

Note: Prior to configuring an AutoIKE VPN that uses digital certificates, you must add the CA and local certificates to the FortiGate unit. For information about digital certificates, see "Managing digital certificates" on page 190.

1. Add the phase 1 parameters. See "Adding a phase 1 configuration for an AutoIKE VPN" on page 183.
2. Add the phase 2 parameters. See "Adding a phase 2 configuration for an AutoIKE VPN" on page 188.
3. Configure an encrypt policy that includes the tunnel, source address, and destination address for both ends of the tunnel. See "Configuring encrypt policies" on page 193.

Adding a phase 1 configuration for an AutoIKE VPN

When you add a phase 1 configuration, you define the terms by which the FortiGate unit and a remote VPN peer (gateway or client) authenticate themselves to each other prior to establishing an IPSec VPN tunnel.

The phase 1 configuration is related to the phase 2 configuration. In phase 1 the VPN peers are authenticated; in phase 2 the tunnel is established. You have the option to use the same phase 1 parameters to establish multiple tunnels. In other words, the same remote VPN peer (gateway or client) can have multiple tunnels to the local VPN peer (the FortiGate unit).

When the FortiGate unit receives an IPSec VPN connection request, it authenticates the VPN peers according to the phase 1 parameters. Then, depending on the source and destination addresses of the request, it starts an IPSec VPN tunnel and applies an encrypt policy.

To add a phase 1 configuration

1. Go to **VPN > IPSEC > Phase 1**.
2. Select New to add a new phase 1 configuration.
3. Type a Gateway Name for the remote VPN peer.
   The remote VPN peer can be either a gateway to another network or an individual client on the Internet.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

4 Select a Remote Gateway address type.

- If the remote VPN peer has a static IP address, select Static IP Address.
- If the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE), or if the remote VPN peer has a static IP address that is not required in the peer identification process, select Dialup User.

Depending on the Remote Gateway address type you selected, other fields become available.

Remote Gateway: Static IP Address

IP Address	If you select Static IP Address, the IP Address field appears. Enter the IP address of the remote IPSec VPN gateway or client that can connect to the FortiGate unit. This is a mandatory entry.

Remote Gateway: Dialup User

Peer Options	If you select Dialup User, the Peer Options become available under Advanced Options. Use the Peer Options to authenticate remote VPN peers with peer IDs during phase 1 negotiations.

5 Select Aggressive or Main (ID Protection) mode.

When using aggressive mode, the VPN peers exchange identifying information in the clear. When using main mode, identifying information is hidden.

The VPN peers must use the same mode.

6 Configure the P1 Proposal.

Select up to three encryption and authentication algorithm combinations to propose for phase 1.

The VPN peers must use the same P1 proposal settings.

7 Select the DH Group(s).

Select one or more Diffie-Hellman groups to propose for phase 1.

As a general rule, the VPN peers should use the same DH Group settings.

8 Enter the Keylife.

The keylife is the amount of time in seconds before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service. P1 proposal keylife can be from 120 to 172,800 seconds.

9 For Authentication Method, select Preshared Key or RSA Signature.

- Preshared Key: Enter a key that is shared by the VPN peers. The key must contain at least 6 printable characters and should only be known by network administrators. For optimum protection against currently known attacks, make sure the key consists of a minimum of 16 randomly chosen alphanumeric characters.
- RSA Signature: Select a local certificate that has been digitally signed by the certificate authority (CA). To add a local certificate to the FortiGate unit, see “Obtaining a signed local certificate” on page 190.

10 Configure the Local ID the that the FortiGate unit sends to the remote VPN peer.

- Preshared key: If the FortiGate unit is functioning as a client and uses its ID to authenticate itself to the remote VPN peer, enter an ID. If no ID is specified, the FortiGate unit transmits its IP address.
- RSA Signature: No entry is required because the Local ID field contains the Distinguished Name (DN) of the certificate associated with this phase 1 configuration. The DN identifies the owner of the certificate and includes, as a minimum, a Common Name (CN). The DN is transmitted in place of an ID or IP address.

Configuring advanced options

To configure phase 1 advanced options

1 Select Advanced Options.

2 Select a Peer Option if you want to authenticate remote VPN peers by the ID that they transmit during phase 1.

Accept any peer ID	Select to accept any peer ID (and therefore not authenticate remote VPN peers by peer ID).
Accept this peer ID	Select to authenticate a specific VPN peer or a group of VPN peers with a shared user name (ID) and password (pre-shared key). Also add the peer ID.
Accept peer ID in dialup group	Select to authenticate each remote VPN peer with a unique user name (ID) and password (pre-shared key). Also select a dialup group (user group). Configure the user group prior to configuring this peer option.

3 Optionally, configure XAuth.

XAuth (IKE eXtended Authentication) authenticates VPN peers at the user level. If the the FortiGate unit (the local VPN peer) is configured as an XAuth server, it authenticates remote VPN peers by referring to a user group. The users contained in the user group can be configured locally on the FortiGate unit or on remotely located LDAP or RADIUS servers. If the FortiGate unit is configured as an XAuth client, it provides a user name and password when it is challenged.

XAuth: Enable as a Client

Name	Enter the user name the local VPN peer uses to authenticate itself to the remote VPN peer.
Password	Enter the password the local VPN peer uses to authenticate itself to the remote VPN peer.

XAuth: Enable as a Server

Encryption method	Select the encryption method used between the XAuth client, the FortiGate unit and the authentication server. **PAP**— Password Authentication Protocol. **CHAP**—Challenge-Handshake Authentication Protocol. **MIXED**—Select MIXED to use PAP between the XAuth client and the FortiGate unit, and CHAP between the FortiGate unit and the authentication server. Use CHAP whenever possible. Use PAP if the authentication server does not support CHAP. (Use PAP with all implementations of LDAP and some implementations of Microsoft RADIUS). Use MIXED if the authentication server supports CHAP but the XAuth client does not. (Use MIXED with the Fortinet Remote VPN Client.).
Usergroup	Select a group of users to be authenticated by XAuth. The individual users within the group can be authenticated locally or by one or more LDAP or RADIUS servers. The user group must be added to the FortiGate configuration before it can be selected here.

4 Optionally, configure NAT Traversal.

Enable	Select Enable if you expect the IPSec VPN traffic to go through a gateway that performs NAT. If no NAT device is detected, enabling NAT traversal has no effect. Both ends of the VPN (both VPN peers) must have the same NAT traversal setting.
Keepalive Frequency	If you enable NAT-traversal, you can change the number of seconds in the Keepalive Frequency field. This number specifies, in seconds, how frequently empty UDP packets are sent through the NAT device to ensure that the NAT mapping does not change until P1 and P2 keylife expires. The keepalive frequency can be from 0 to 900 seconds.

5 Optionally, configure Dead Peer Detection.

Use these settings to monitor the status of the connection between VPN peers. DPD allows dead connections to be cleaned up and new VPN tunnels established. DPD is not supported by all vendors.

Enable	Select Enable to enable DPD between the local and remote peers.
Short Idle	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 also sends a DPD probe to determine the status of the link. To control the length of time that the FortiGate unit takes to detect a dead peer with DPD probes, configure the Retry Count and the Retry Interval.
Retry Count	Set the number of times that the local VPN peer retries the DPD probe before it considers the channel to be dead and tears down the security association (SA). To avoid false negatives because of congestion or other transient failures, set the retry count to a sufficiently high value for your network.
Retry Interval	Set the time, in seconds, that the local VPN peer unit waits between retrying DPD probes.
Long Idle	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 sends a DPD probe to determine the status of the link even if there is no traffic between the local peer and the remote peer.

6 Select OK to save the phase 1 parameters.

Figure 21: Adding a phase 1 configuration (Standard options)

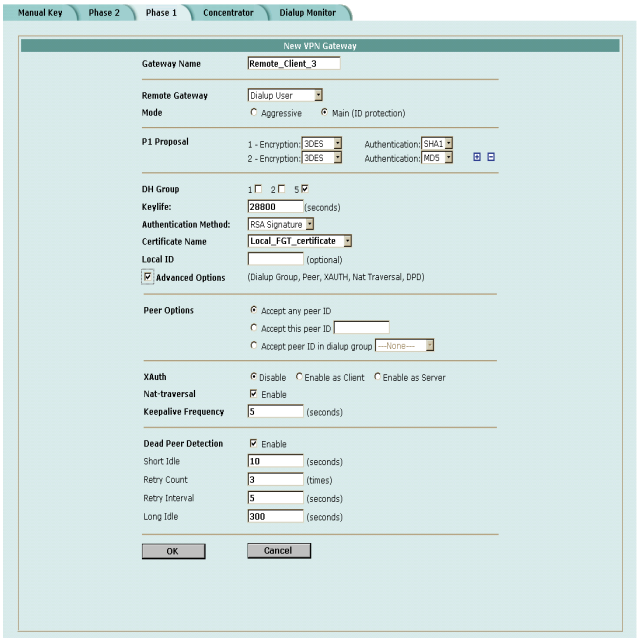
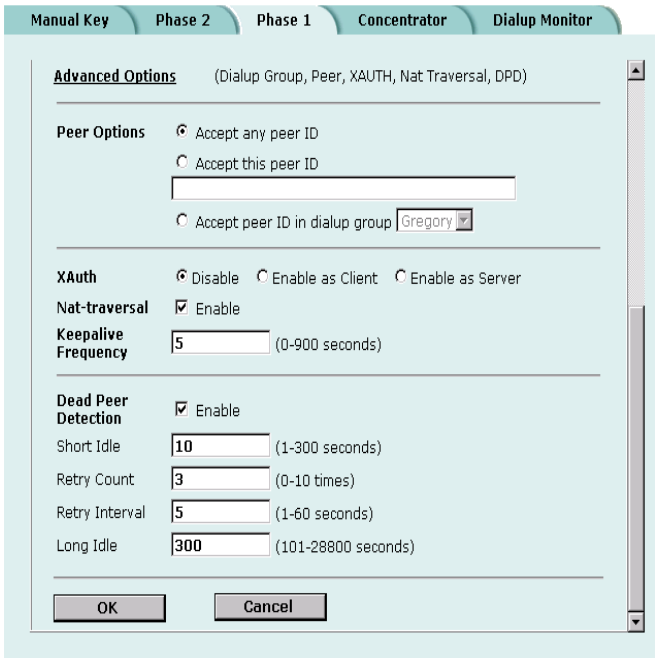


Figure 22: Adding a phase 1 configuration (Advanced options)



Adding a phase 2 configuration for an AutoIKE VPN

Add a phase 2 configuration to specify the parameters used to create and maintain a VPN tunnel between the local VPN peer (the FortiGate unit) and the remote VPN peer (the VPN gateway or client).

Note: Adding a Phase 2 configuration is the same for pre-shared key and certification VPNs.

To add a phase 2 configuration

1. Go to **VPN > IPSEC > Phase 2**.
2. Select New to add a new phase 2 configuration.
3. Enter a Tunnel Name.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Select a Remote Gateway to associate with the VPN tunnel.
   A remote gateway can be either a gateway to another network or an individual client on the Internet. Remote gateways are added as part of the phase 1 configuration. For details, see “Adding a phase 1 configuration for an AutoIKE VPN” on page 183.
   Choose either a single DIALUP remote gateway, or up to three STATIC remote gateways. Multiple STATIC remote gateways are necessary if you are configuring IPSec redundancy.
5. Configure the P2 Proposal.
   Select up to three encryption and authentication algorithm combinations to propose for phase 2.
   The VPN peers must use the same P2 proposal settings.
6. Optionally, enable Replay Detection.
   Replay detection protects the VPN tunnel from replay attacks.

Note: Do not select replay detection if you have also selected Null Authentication for the P2 Proposal.

7. Optionally, enable Perfect Forward Secrecy (PFS).
   PFS improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
8. Select the DH Group(s).
   The VPN peers must use the same DH Group settings.
9. Enter the Keylife.
   The keylife causes the phase 2 key to expire after a specified time, after a specified number of Kbytes of data have been processed by the VPN tunnel, or both. If you select both, the key does not expire until both the time has passed and the number of Kbytes have been processed.
   When the key expires, a new key is generated without interrupting service. P2 proposal keylife can be from 120 to 172800 seconds or from 5120 to 99999 Kbytes.

10 Enable Autokey Keep Alive if you want to keep the VPN tunnel running even if no data is being processed.

11 Select a concentrator if you want the tunnel to be part of a hub and spoke VPN configuration.

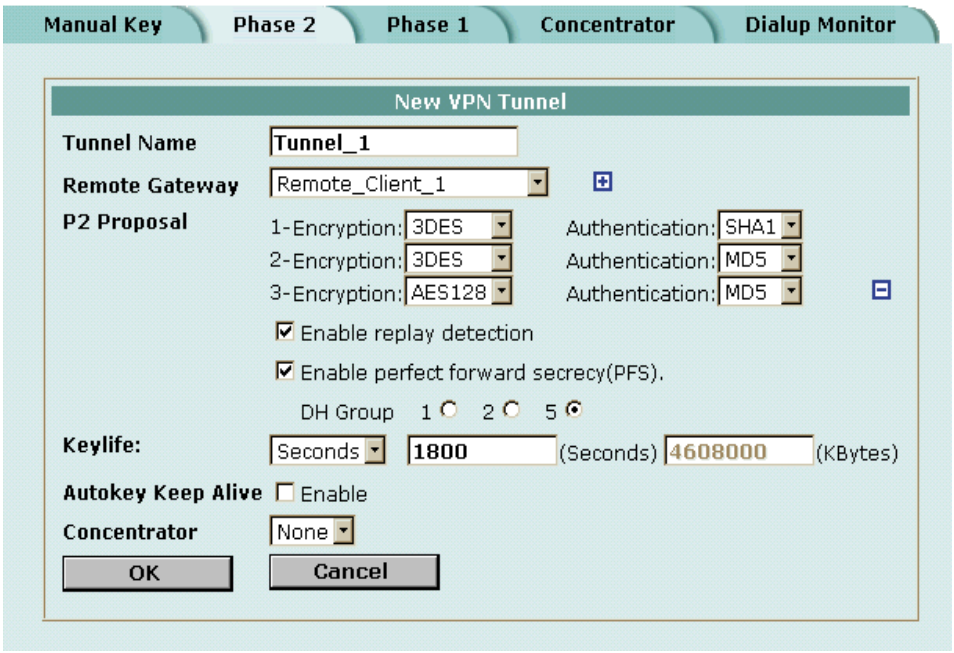
If you use the procedure, "Adding a VPN concentrator" on page 198 to add the tunnel to a concentrator, the next time you open the tunnel, the Concentrator field displays the name of the concentrator to which you added the tunnel.

12 Select a Quick Mode Identity.

Use selectors from policy	Select this option for policy-based VPNs. A policy-based VPN uses an encrypt policy to select which VPN tunnel to use for the connection. In this configuration, the VPN tunnel is referenced directly from the encrypt policy. You must select this option if both VPN peers are FortiGate units.
Use wildcard selectors	Select this option for routing-based VPNs. A routing-based VPN uses routing information to select which VPN tunnel to use for the connection. In this configuration, the tunnel is referenced indirectly by a route that points to a tunnel interface. You must select this option if the remote VPN peer is a non-FortiGate unit that has been configured to operate in tunnel interface mode.

13 Select OK to save the AutoIKE key VPN tunnel.

Figure 23: Adding a phase 2 configuration



Managing digital certificates

Use digital certificates to make sure that both participants in an IPSec communication session are trustworthy, prior to setting up an encrypted VPN tunnel between the participants.

Fortinet uses a manual procedure to obtain certificates. This involves copying and pasting text files from your local computer to the certificate authority, and from the certificate authority to your local computer.

- Obtaining a signed local certificate
- Obtaining CA certificates

Note: Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Obtaining a signed local certificate

The signed local certificate provides the FortiGate unit with a means to authenticate itself to other devices.

Note: The VPN peers must use digital certificates that adhere to the X.509 standard.

Generating the certificate request

With this procedure, you generate a private and public key pair. The public key is the base component of the certificate request.

To generate the certificate request

1. Go to **VPN > Certificates > Local Certificates**.
2. Select Generate.
3. Type a Certificate Name.
   The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
4. Configure the Subject Information that identifies the object being certified.
   Preferably use an IP address or domain name. If this is impossible (such as with a dialup client), use an email address.

Host IP	For Host IP, enter the IP address of the FortiGate unit being certified.
Domain Name	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.
E-Mail	For E-mail, enter the email address of the owner of the FortiGate unit being certified. Typically, e-mail addresses are entered only for clients, not gateways.

5. Configure the Optional Information to further identify the object being certified.

Organization Unit	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiGate unit (such as Manufacturing or MF).
Organization	Enter the legal name of the organization that is requesting the certificate for the FortiGate unit (such as Fortinet).
Locality	Enter the name of the city or town where the FortiGate unit is located (such as Vancouver).
State/Province	Enter the name of the state or province where the FortiGate unit is located (such as California or CA).
Country	Select the country where the FortiGate unit is located.
e-mail	Enter a contact email address for the FortiGate unit. Typically, email addresses are entered only for clients, not gateways.

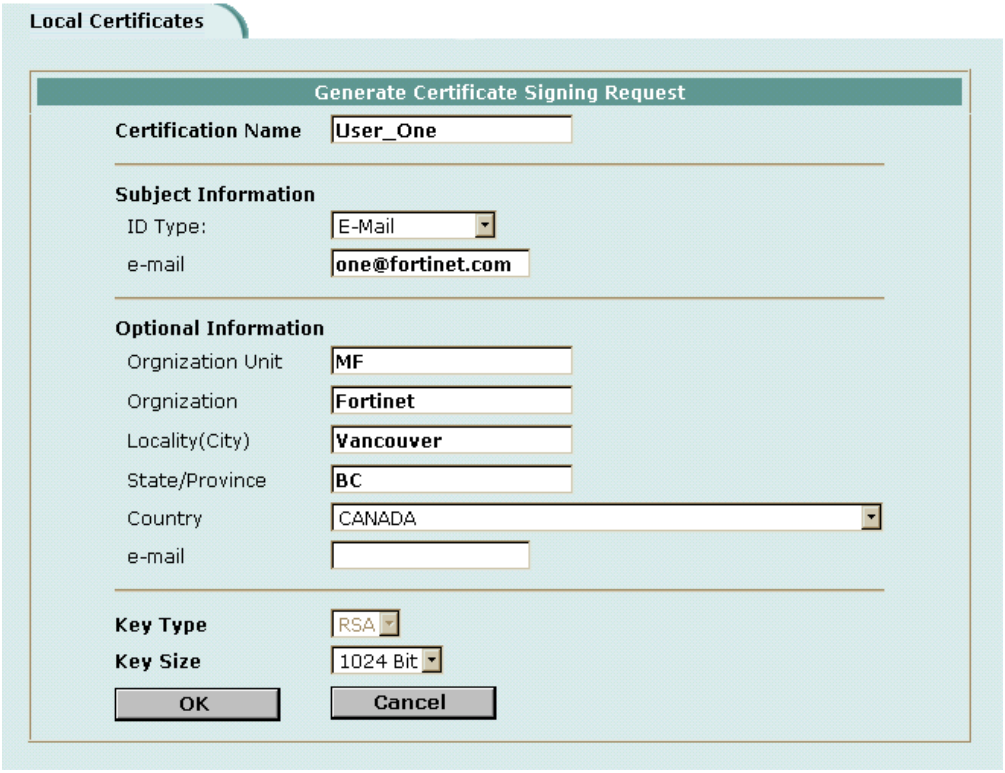
6 Configure the key.

Key Type	Select RSA as the key encryption type. No other key type is supported.
Key Size	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.

7 Select OK to generate the private and public key pair and the certificate request.

The private/public key pair are generated and the certificate request is displayed on the Local Certificates list with a status of Pending.

Figure 24: Adding a Local Certificate



Downloading the certificate request

Use the following procedure to download a certificate request from the FortiGate unit to the management computer.

To download the certificate request

1. Go to **VPN > Certificates > Local Certificates**.
2. Select Download to download the local certificate to the management computer.
3. Select Save.
4. Name the file and save it in a directory on the management computer.

   After downloading the certificate request, you can submit it tor your CA so that your CA can sign the certificate.

Importing the signed local certificate

With this procedure, you import the signed local certificate from the management computer to the FortiGate unit.

To import the signed local certificate

1. Go to **VPN > Certificates > Local Certificates**.
2. Select Import.
3. Enter the path or browse to locate the signed local certificate on the management computer.
4. Select OK.

   The signed local certificate is displayed on the Local Certificates list with a status of OK.

Backing up and restoring the local certificate and private key

When you back up a FortiGate configuration that includes IPSec VPN tunnels using certificates, you must also back up the local certificate and private key in a password-protected PKCS12 file. Before restoring the configuration, you must import the PKCS12 file and set the local certificate name to the same that was in the original configuration.

Public Key Cryptography Standard 12 (PKCS12) describes the syntax for securely exchanging personal information.

Note: Use the `execute vpn certificates key` CLI command to back up and restore the local certificate and private key. For more information, see the *FortiGate CLI Reference Guide*.

Obtaining CA certificates

For the VPN peers to authenticate themselves to each other, they must both obtain a CA certificate from the same certificate authority. The CA certificate provides the VPN peers with a means to validate the digital certificates that they receive from other devices.

The FortiGate unit obtains the CA certificate to validate the digital certificate that it receives from the remote VPN peer. The remote VPN peer obtains the CA certificate to validate the digital certificate that it receives from the FortiGate unit.

Note: The CA certificate must adhere to the X.509 standard.

Importing CA certificates

Import the CA certificate from the management computer to the FortiGate unit.

To import the CA certificate

1. Go to **VPN > Certificates > CA Certificates**.
2. Select Import.
3. Enter the path or browse to locate the CA certificate on the management computer.
4. Select OK.
   The CA is displayed on the CA Certificates list.
   The system assigns a unique name to each CA certificate. The names are numbered consecutively (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on).

Configuring encrypt policies

A VPN connects the local, internal network to a remote, external network. The principal role of the encrypt policy is to define (and limit) which addresses on these networks can use the VPN.

A VPN requires only one encrypt policy to control both inbound and outbound connections. Depending on how you configure it, the policy controls whether users on your internal network can establish a tunnel to the remote network (the outbound connection), and whether users on the remote network can establish a tunnel to your internal network (the inbound connection). This flexibility allows one encrypt policy to do the same function as two regular firewall policies.

Although the encrypt policy controls both incoming and outgoing connections, it must always be configured as an outgoing policy. An outgoing policy has a source address on an internal network and a destination address on an external network. The source address identifies the addresses on the internal network that are part of the VPN. The destination address identifies the addresses on the remote network that are part of the VPN.

Note: The destination address can be a VPN client address on the Internet or the address of a network behind a remote VPN gateway.

In addition to defining membership in the VPN by address, you can configure the encrypt policy for services such as DNS, FTP, and POP3, and to allow connections according to a predefined schedule (by the time of the day or the day of the week, month, or year). You can also configure the encrypt policy for:

- Inbound NAT to translate the source of incoming packets.
- Outbound NAT to translate the source address of outgoing packets.
- Traffic shaping to control the bandwidth available to the VPN and the priority of the VPN.
- Content profiles to apply antivirus protection, web filtering, and email filtering to web, file transfer, and email services in the VPN.
- Logging so that the FortiGate unit logs all connections that use the VPN.

The policy must also include the VPN tunnel that you created to communicate with the remote FortiGate VPN gateway. When users on your internal network attempt to connect to the network behind the remote VPN gateway, the encrypt policy intercepts the connection attempt and starts the VPN tunnel added to the policy. The tunnel uses the remote gateway added to its configuration to connect to the remote VPN gateway. When the remote VPN gateway receives the connection attempt, it checks its own policy, gateway, and tunnel configuration. If the configuration is allowed, an IPSec VPN tunnel is negotiated between the two VPN peers.

- Adding a source address
- Adding a destination address
- Adding an encrypt policy

Adding a source address

The source address is located within the internal network of the local VPN peer. It can be a single computer address or the address of a network.

To add a source address

1. Go to **Firewall > Address**.
2. Select an internal interface.
3. Select New to add an address.
4. Enter the Address Name, IP Address, and NetMask for a single computer or for an entire subnetwork on an internal interface of the local VPN peer.
5. Select OK to save the source address.

Adding a destination address

The destination address can be a VPN client address on the Internet or the address of a network behind a remote VPN gateway.

To add a destination address

1. Go to **Firewall > Address**.
2. Select an external interface.
3. Select New to add an address.

4 Enter the Address Name, IP Address, and NetMask for a single computer or for an entire subnetwork on an internal interface of the remote VPN peer.

5 Select OK to save the destination address.

Adding an encrypt policy

To add an encrypt policy

1 Go to **Firewall > Policy**.

2 Select the Int->Ext policy list.

3 Select New to add a new policy.

4 Set Source to the source address.

5 Set Destination to the destination address.

6 Set Service to control the services allowed over the VPN connection.

You can select ANY to allow all supported services over the VPN connection or select a specific service or service group to limit the services allowed over the VPN connection.

7 Set Action to ENCRYPT.

8 Configure the ENCRYPT parameters.

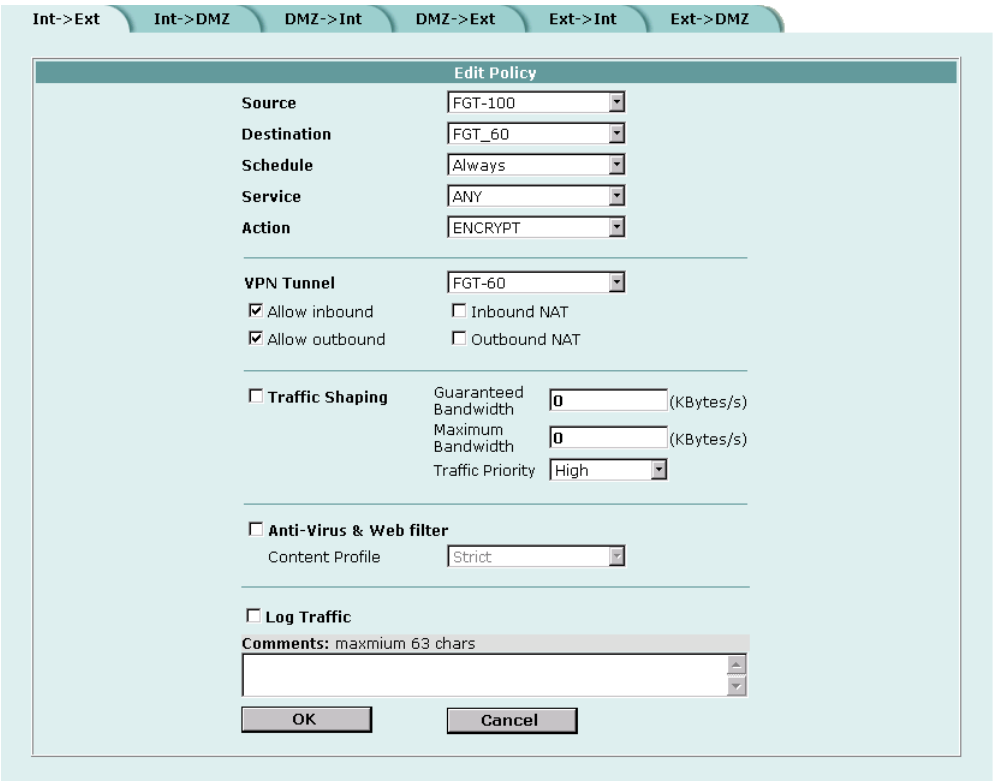
VPN Tunnel	Select an Auto Key tunnel for this encrypt policy.
Allow inbound	Select Allow inbound to enable inbound users to connect to the source address.
Allow outbound	Select Allow outbound to enable outbound users to connect to the destination address.
Inbound NAT	The FortiGate unit translates the source address of incoming packets to the IP address of the FortiGate interface connected to the source address network. Typically, this is an internal interface of the FortiGate unit. Inbound NAT makes it impossible for local hosts to see the IP addresses of remote hosts (hosts located on the network behind the remote VPN gateway).
Outbound NAT	The FortiGate unit translates the source address of outgoing packets to the IP address of the FortiGate interface connected to the destination address network. Typically, this is an external interface of the FortiGate unit. Outbound NAT makes it impossible for remote hosts to see the IP addresses of local hosts (hosts located on the network behind the local VPN gateway). If Outbound NAT is implemented, it is subject to these limitations: Configure Outbound NAT only at one end of the tunnel. The end that does not implement Outbound NAT requires an internal to external policy that specifies the remote external interface as the Destination (usually a public IP address). The tunnel, and the traffic within the tunnel, can only be initiated at the end that implements Outbound NAT.

For information about configuring the remaining policy settings, see “Adding firewall policies” on page 140.

9 Select OK to save the encrypt policy.

To make sure that the encrypt policy is matched for VPN connections, arrange the encrypt policy above other policies with similar source and destination addresses and services in the policy list.

Figure 25: Adding an encrypt policy



IPSec VPN concentrators

In a hub-and-spoke network, all VPN tunnels terminate at a single VPN peer called a hub. The peers that connect to the hub are known as spokes. The hub functions as a concentrator on the network, managing the VPN connections between the spokes.

The advantage of a hub-and-spoke network is that the spokes are simpler to configure because they require fewer policy rules. Also, a hub-and-spoke network provides some processing efficiencies, particularly on the spokes. The disadvantage of a hub-and-spoke network is its reliance on a single peer to handle management of all VPNs. If this peer fails, encrypted communication in the network is impossible.

A hub-and-spoke VPN network requires a special configuration. Setup varies depending on the role of the VPN peer.

If the VPN peer is a FortiGate unit functioning as the hub, or concentrator, it requires a VPN configuration connecting it to each spoke (AutoIKE phase 1 and 2 settings or manual key settings, plus encrypt policies). It also requires a concentrator configuration that groups the hub-and-spoke tunnels together. The concentrator configuration defines the FortiGate unit as the hub in a hub-and-spoke network.

If the VPN peer is one of the spokes, it requires a tunnel connecting it to the hub (but not to the other spokes). It also requires policies that control its encrypted connections to the other spokes and its non-encrypted connections to other networks, such as the Internet.

VPN concentrator (hub) general configuration steps

A central FortiGate that is functioning as a hub requires the following configuration:

- A tunnel (AutoIKE phase 1 and phase 2 configuration or manual key configuration) for each spoke.
- Destination addresses for each spoke.
- A concentrator configuration.
- An encrypt policy for each spoke.

To create a VPN concentrator configuration

1. Configure one of the following tunnels for each spoke:
   - A manual key tunnel consists of a name for the tunnel, the IP address of the spoke (client or gateway) at the opposite end of the tunnel, and the encryption and authentication algorithms to use for the tunnel.

     See “Manual key IPSec VPNs” on page 181.
   - An AutoIKE tunnel consists of phase 1 and phase 2 parameters. The phase 1 parameters include the name of the spoke (client or gateway), designation of how the spoke receives its IP address (static or dialup), encryption and authentication algorithms, and the authentication method (either pre-shared keys or PKI certificates). The phase 2 parameters include the name of the tunnel, selection of the spoke (client or gateway) configured in phase 1, encryption and authentication algorithms, and a number of security parameters.

     See “AutoIKE IPSec VPNs” on page 182.
2. Add a destination address for each spoke. The destination address is the address of the spoke (either a client on the Internet or a network located behind a gateway).

   See “Adding a source address” on page 194.
3. Add the concentrator configuration. This step groups the tunnels together on the FortiGate unit. The tunnels link the hub to the spokes. The tunnels are added as part of the AutoIKE phase 2 configuration or the manual key configuration.

   See “Adding a VPN concentrator” on page 198.

Note: Add the concentrator configuration to the central FortiGate unit (the hub) after adding the tunnels for all spokes.

4 Add an encrypt policy for each spoke. Encrypt policies control the direction of traffic through the hub and allow inbound and outbound VPN connections between the hub and the spokes. The encrypt policy for each spoke must include the tunnel name of the spoke. The source address must be Internal_All. Use the following configuration for the encrypt policies:

Source	Internal_All
Destination	The VPN spoke address.
Action	ENCRYPT
VPN Tunnel	The VPN spoke tunnel name.
Allow inbound	Select allow inbound.
Allow outbound	Select allow outbound
Inbound NAT	Select inbound NAT if required.
Outbound NAT	Select outbound NAT if required.

See “Adding an encrypt policy” on page 195.

5 Arrange the policies in the following order:
- encrypt policies
- default non-encrypt policy (Internal_All -> External_All)

Adding a VPN concentrator

To add a VPN concentrator configuration

1 Go to **VPN > IPSec > Concentrator**.

2 Select New to add a VPN concentrator.

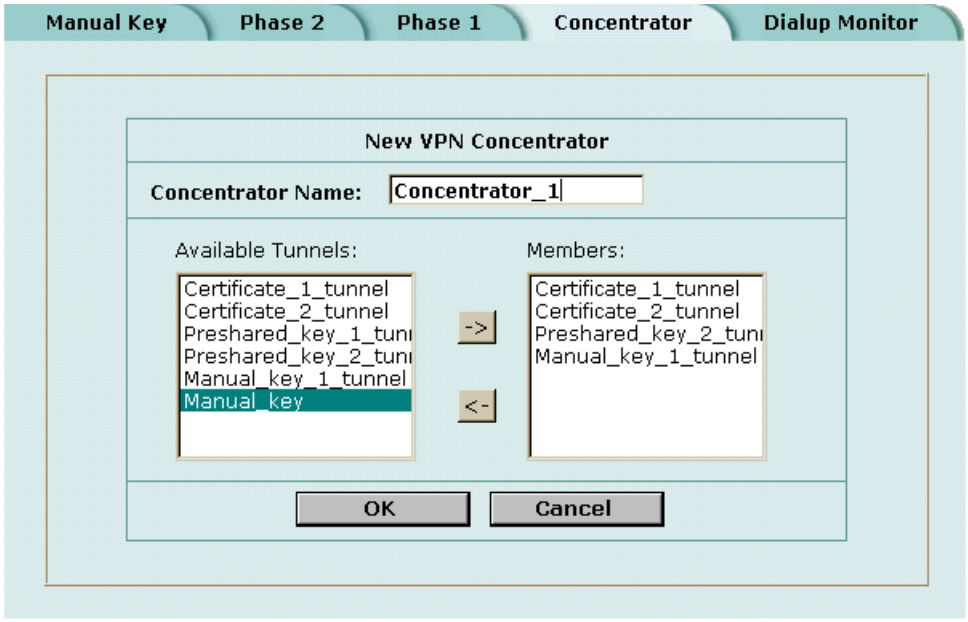
3 Enter the name of the new concentrator in the Concentrator Name field.

4 To add tunnels to the VPN concentrator, select a VPN tunnel from the Available Tunnels list and select the right arrow.

5 To remove tunnels from the VPN concentrator, select the tunnel in the Members list and select the left arrow.

6 Select OK to add the VPN concentrator.

Figure 26: Adding a VPN concentrator



VPN spoke general configuration steps

A remote VPN peer that functions as a spoke requires the following configuration:

- A tunnel (AutoIKE phase 1 and phase 2 configuration or manual key configuration) for the hub.
- The source address of the local VPN spoke.
- The destination address of each remote VPN spoke.
- A separate outbound encrypt policy for each remote VPN spoke. These policies allow the local VPN spoke to initiate encrypted connections.
- A single inbound encrypt policy. This policy allows the local VPN spoke to accept encrypted connections.

To create a VPN spoke configuration

1 Configure a tunnel between the spoke and the hub.

Choose between a manual key tunnel or an AutoIKE tunnel.

- To add a manual key tunnel, see “Manual key IPSec VPNs” on page 181.
- To add an AutoIKE tunnel, see “AutoIKE IPSec VPNs” on page 182.

2 Add the source address. One source address is required for the local VPN spoke.

See “Adding a source address” on page 194.

3 Add a destination address for each remote VPN spoke. The destination address is the address of the spoke (either a client on the Internet or a network located behind a gateway).

See “Adding a destination address” on page 194

4 Add a separate outbound encrypt policy for each remote VPN spoke. These policies control the encrypted connections initiated by the local VPN spoke.

The encrypt policy must include the appropriate source and destination addresses and the tunnel added in step 1. Use the following configuration:

Source	The local VPN spoke address.
Destination	The remote VPN spoke address.
Action	ENCRYPT
VPN Tunnel	The VPN tunnel name added in step 1. (Use the same tunnel for all encrypt policies.)
Allow inbound	Do not enable.
Allow outbound	Select allow outbound
Inbound NAT	Select inbound NAT if required.
Outbound NAT	Select outbound NAT if required.

See “Adding an encrypt policy” on page 195.

5 Add an inbound encrypt policy. This policy controls the encrypted connections initiated by the remote VPN spokes.

The encrypt policy for the hub must include the appropriate source and destination addresses and the tunnel added in step 1. Use the following configuration:

Source	The local VPN spoke address.
Destination	External_All
Action	ENCRYPT
VPN Tunnel	The VPN tunnel name added in step 1. (Use the same tunnel for all encrypt policies.)
Allow inbound	Select allow inbound.
Allow outbound	Do not enable.
Inbound NAT	Select inbound NAT if required.
Outbound NAT	Select outbound NAT if required.

See “Adding an encrypt policy” on page 195.

6 Arrange the policies in the following order:

- outbound encrypt policies
- inbound encrypt policy
- default non-encrypt policy (Internal_All -> External_All)

Note: The default non-encrypt policy is required to allow the VPN spoke to access other networks, such as the Internet.

Monitoring and Troubleshooting VPNs

Viewing VPN tunnel status

You can use the IPSec VPN tunnel list to view the status of all IPSec AutoIKE key VPN tunnels. For each tunnel, the list shows the status and the tunnel time out.

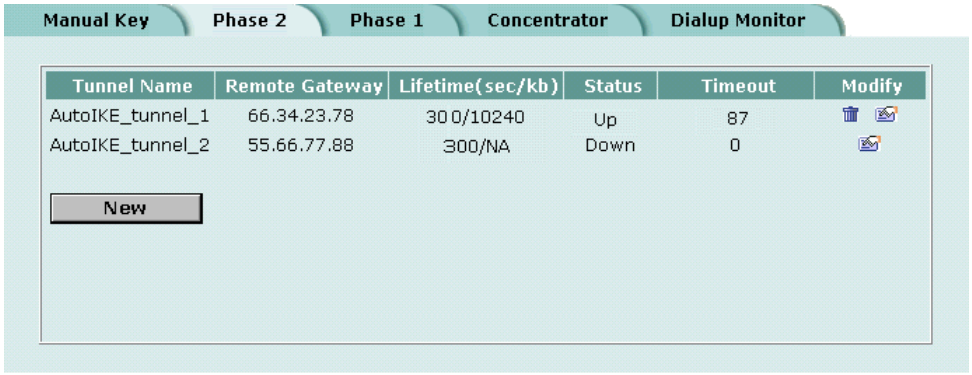
To view VPN tunnel status

1 Go to **VPN > IPSEC > Phase 2**.

2 View the status and timeout for each VPN tunnel.

Status	The status of each tunnel. If Status is Up, the tunnel is active. If Status is Down, the tunnel is not active. If Status is Connecting, the tunnel is attempting to start a VPN connection with a remote VPN gateway or client.
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.

Figure 27: AutoIKE key tunnel status



Viewing dialup VPN connection status

You can use the dialup monitor to view the status of dialup VPNs. The dialup monitor lists the remote gateways and the active VPN tunnels for each gateway. The monitor also lists the tunnel lifetime, timeout, proxy ID source, and proxy ID destination for each tunnel.

To view dialup connection status

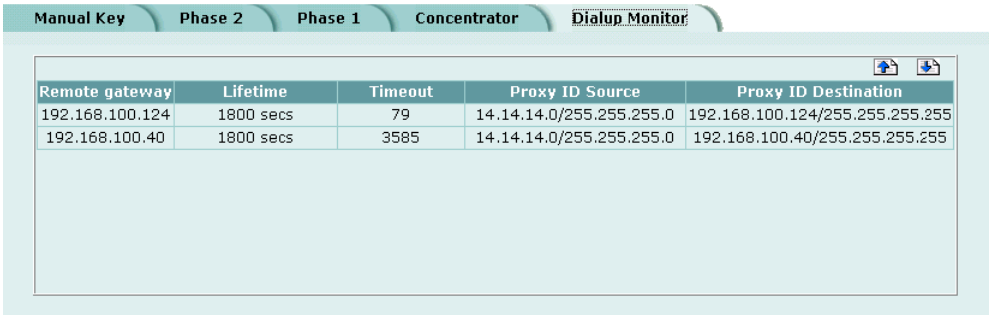
1 Go to **VPN > IPSec > Dialup Monitor**.

2 View the dialup connection status information for the FortiGate unit:

Remote gateway	The IP address of the remote dialup remote gateway on the FortiGate unit.
Lifetime	The amount of time that the dialup VPN connection has been active.
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 actual IP address or subnet address of the remote peer.
Proxy ID Destination	The actual IP address or subnet address of the local peer.

Figure 28: Dialup Monitor



Testing a VPN

To confirm that a VPN between two networks has been configured correctly, use the ping command from one internal network to connect to a computer on the other internal network. The IPSec VPN tunnel starts automatically when the first data packet destined for the VPN is intercepted by the FortiGate unit.

To confirm that a VPN between a network and one or more clients has been configured correctly, start a VPN client and use the ping command to connect to a computer on the internal network. The VPN tunnel initializes automatically when the client makes a connection attempt. You can start the tunnel and test it at the same time by pinging from the client to an address on the internal network.

PPTP and L2TP VPN

You can use PPTP and L2TP to create a virtual private network (VPN) between a remote client computer that is running Windows and your internal network. Because PPTP and L2TP are supported by Windows you do not require third-party software on the client computer. Provided your ISP supports PPTP and L2TP connections, you can create a secure connection by making some configuration changes to the client computer and the FortiGate unit.

This chapter provides an overview of how to configure FortiGate PPTP and L2TP VPN. For a complete description of FortiGate PPTP and L2TP, see the *FortiGate VPN Guide*.

This chapter describes:

Configuring PPTP

Point-to-Point protocol (PPTP) packages data within PPP packets and then encapsulates the PPP packets within IP packets for transmission through a VPN tunnel.

Note: PPTP VPNs are supported only in NAT/Route mode.

This section describes:

Configuring the FortiGate unit as a PPTP gateway

Use the following procedures to configure the FortiGate unit as a PPTP gateway:

To add users and user groups

Add a user for each PPTP client.

1 Go to **User > Local**.

2 Add and configure PPTP users.
For information about adding and configuring users, see “Adding user names and configuring authentication” on page 172.

3 Go to **User > User Group**.

4 Add and configure PPTP user groups.
For information about adding and configuring user groups, see “Configuring user groups” on page 177.

To enable PPTP and specify an address range

1 Go to **VPN > PPTP > PPTP Range**.

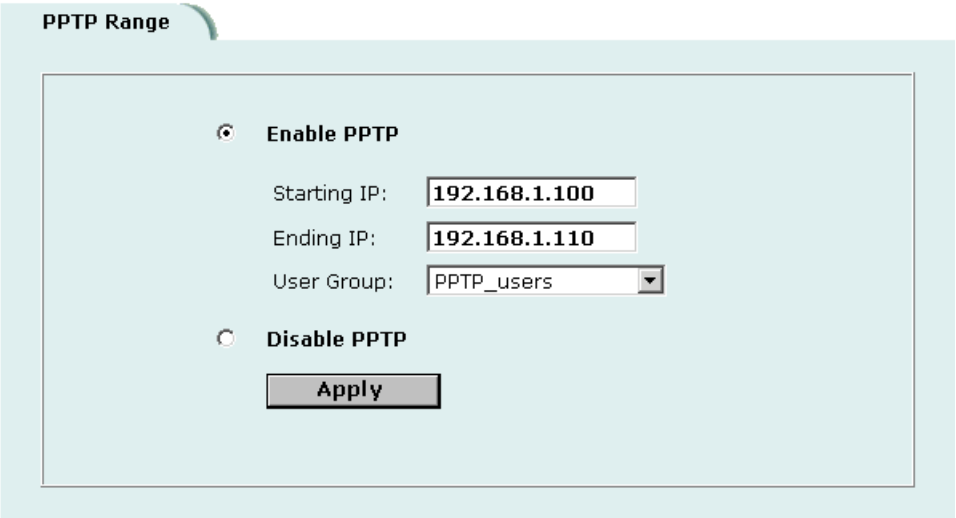
2 Select Enable PPTP.

3 Enter the Starting IP and the Ending IP for the PPTP address range.

4 Select the User Group that you added in “To add users and user groups” on page 203.

5 Select Apply to enable PPTP through the FortiGate unit.

Figure 29: Example PPTP Range configuration



To add a source address

Add a source address for every address in the PPTP address range.

1 Go to **Firewall > Address**.

2 Select the interface to which PPTP clients connect.

3 Select New to add an address.

4 Enter the Address Name, IP Address, and NetMask for an address in the PPTP address range.

5 Select OK to save the source address.

6 Repeat for all addresses in the PPTP address range.

Note: If the PPTP address range is comprised of an entire subnet, add an address for this subnet. Do not add an address group.

To add a source address group

Organize the source addresses into an address group.

1 Go to **Firewall > Address > Group**.

2 Add a new address group to the interface to which PPTP clients connect.

3 Enter a Group Name to identify the address group.
The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

4 To add addresses to the address group, select an address from the Available Addresses list and select the right arrow to add it to the Members list.

5 To remove addresses from the address group, select an address from the Members list and select the left arrow to remove it from the group.

6 Select OK to add the address group.

To add a destination address

Add an address to which PPTP users can connect.

1 Go to **Firewall > Address**.

2 Select the internal interface.

3 Select New to add an address.

4 Enter the Address Name, IP Address, and NetMask for a single computer or for an entire subnetwork on an internal interface of the local VPN peer.

5 Select OK to save the destination address.

To add a firewall policy

Add a policy which specifies the source and destination addresses and sets the service for the policy to the traffic type inside the PPTP VPN tunnel.

1 Go to **Firewall > Policy**.

2 Select the Ext->Int policy list.

3 Select New to add a new policy.

4 Set Source to the group that matches the PPTP address range.

5 Set Destination to the address to which PPTP users can connect.

6 Set Service to match the traffic type inside the PPTP VPN tunnel.
For example, if PPTP users can access a web server, select HTTP.

7 Set Action to ACCEPT.

8 Select NAT if address translation is required.
You can also configure traffic shaping, logging, and antivirus and web filter settings for PPTP policies.

9 Select OK to save the firewall policy.

Configuring a Windows 98 client for PPTP

Use the following procedure to configure a client computer running Windows 98 so that it can connect to a FortiGate PPTP VPN. To configure the Windows 98 client, you must install and configure Windows dialup networking and virtual private networking support.

To install PPTP support

1. Go to **Start > Settings > Control Panel > Network**.
2. Select Add.
3. Select Adapter.
4. Select Add.
5. Select Microsoft as the manufacturer.
6. Select Microsoft Virtual Private Networking Adapter.
7. Select OK twice.
8. Insert diskettes or CDs as required.
9. Restart the computer.

To configure a PPTP dialup connection

1. Go to **My Computer > Dial-Up Networking > Configuration**.
2. Double-click Make New Connection.
3. Name the connection and select Next.
4. Enter the IP address or host name of the FortiGate unit to connect to and select Next.
5. Select Finish.
   An icon for the new connection appears in the Dial-Up Networking folder.
6. Right-click the new icon and select Properties.
7. Go to Server Types.
8. Uncheck IPX/SPX Compatible.
9. Select TCP/IP Settings.
10. Uncheck Use IP header compression.
11. Uncheck Use default gateway on remote network.
12. Select OK twice.

To connect to the PPTP VPN

1. Start the dialup connection that you configured in the previous procedure.
2. Enter your PPTP VPN User Name and Password.
3. Select Connect.

Configuring a Windows 2000 client for PPTP

Use the following procedure to configure a client computer running Windows 2000 so that it can connect to a FortiGate PPTP VPN.

To configure a PPTP dialup connection

1. Go to **Start > Settings > Network and Dial-up Connections**.
2. Double-click Make New Connection to start the Network Connection Wizard and select Next.
3. For Network Connection Type, select Connect to a private network through the Internet and select Next.
4. For Destination Address, enter the IP address or host name of the FortiGate unit to connect to and select Next.
5. Set Connection Availability to Only for myself and select Next.
6. Select Finish.
7. In the Connect window, select Properties.
8. Select the Security tab.
9. Uncheck Require data encryption.
10. Select OK.

To connect to the PPTP VPN

1. Start the dialup connection that you configured in the previous procedure.
2. Enter your PPTP VPN User Name and Password.
3. Select Connect.
4. In the connect window, enter the User Name and Password that you use to connect to your dialup network connection.
   This user name and password is not the same as your VPN user name and password.

Configuring a Windows XP client for PPTP

Use the following procedure to configure a client computer running Windows XP so that it can connect to a FortiGate PPTP VPN.

To configure a PPTP dialup connection

1. Go to **Start > Settings > Control Panel**.
2. Select Network and Internet Connections.
3. Select Create a Connection to the network of your workplace and select Next.
4. Select Virtual Private Network Connection and select Next.
5. Name the connection and select Next.
6. If the Public Network dialog box appears, choose the appropriate initial connection and select Next.
7. In the VPN Server Selection dialog, enter the IP address or host name of the FortiGate unit to connect to and select Next.

8 Select Finish.

To configure the VPN connection

1 Right-click the Connection icon that you created in the previous procedure.

2 Select **Properties > Security**.

3 Select Typical to configure typical settings.

4 Select Require data encryption.

Note: If a RADIUS server is used for authentication do not select Require data encryption. PPTP encryption is not supported for RADIUS server authentication.

5 Select Advanced to configure advanced settings.

6 Select Settings.

7 Select Challenge Handshake Authentication Protocol (CHAP).

8 Make sure that none of the other settings are selected.

9 Select the Networking tab.

10 Make sure that the following options are selected:
- TCP/IP
- QoS Packet Scheduler

11 Make sure that the following options are not selected:
- File and Printer Sharing for Microsoft Networks
- Client for Microsoft Networks

12 Select OK.

To connect to the PPTP VPN

1 Connect to your ISP.

2 Start the VPN connection that you configured in the previous procedure.

3 Enter your PPTP VPN User Name and Password.

4 Select Connect.

5 In the connect window, enter the User Name and Password that you use for your dialup network connection.
This user name and password is not the same as your VPN user name and password.

Configuring L2TP

Some implementations of L2TP support elements of IPSec. These elements must be disabled when L2TP is used with a FortiGate unit.

Note: L2TP VPNs are only supported in NAT/Route mode.

This section describes:

- Configuring the FortiGate unit as an L2TP gateway
- Configuring a Windows 2000 client for L2TP
- Configuring a Windows XP client for L2TP

Configuring the FortiGate unit as an L2TP gateway

Use the following procedures to configure the FortiGate unit as an L2TP gateway:

To add users and user groups

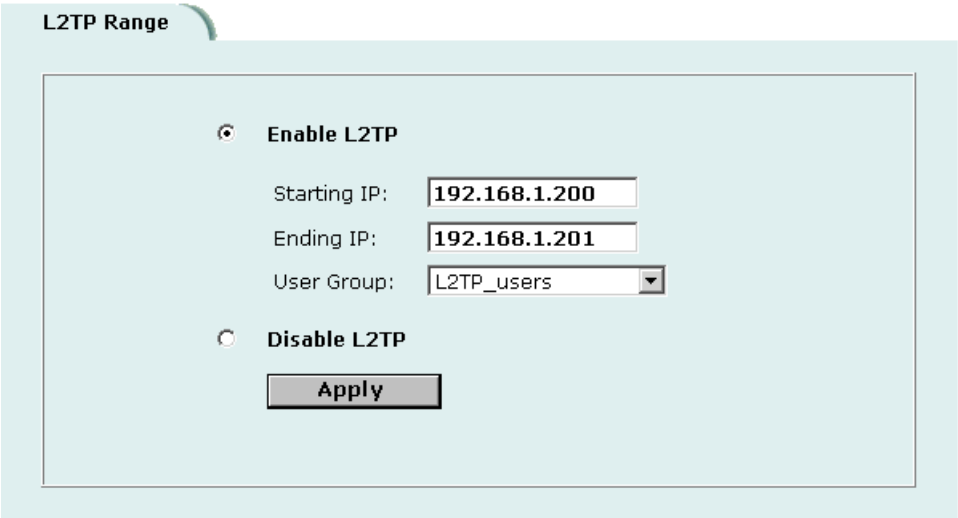
Add a user for each L2TP client.

1. Go to **User > Local**.
2. Add and configure L2TP users.
   See “Adding user names and configuring authentication” on page 172.
3. Go to **User > User Group**.
4. Add and configure L2TP user groups.
   See “Configuring user groups” on page 177.

To enable L2TP and specify an address range

1. Go to **VPN > L2TP > L2TP Range**.
2. Select Enable L2TP.
3. Enter the Starting IP and the Ending IP for the L2TP address range.
4. Select the User Group that you added in “To add users and user groups” on page 209.
5. Select Apply to enable L2TP through the FortiGate unit.

Figure 30: Sample L2TP address range configuration



To add source addresses

Add a source address for every address in the L2TP address range.

1 Go to **Firewall > Address**.

2 Select the interface to which L2TP clients connect.

3 Select New to add an address.

1 Enter the Address Name, IP Address, and NetMask for an address in the L2TP address range.

2 Select OK to save the source address.

3 Repeat for all addresses in the L2TP address range.

Note: If the L2TP address range is comprised of an entire subnet, add an address for this subnet. Do not add an address group.

To add a source address group

Organize the source addresses into an address group.

1 Go to **Firewall > Address > Group**.

2 Add a new address group to the interface to which L2TP clients connect.

3 Enter a Group Name to identify the address group.

The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.

4 To add addresses to the address group, select an address from the Available Addresses list and select the right arrow to add it to the Members list.

5 To remove addresses from the address group, select an address from the Members list and select the left arrow to remove it from the group.

6 Select OK to add the address group.

To add a destination address

Add an address to which L2TP users can connect.

1 Go to **Firewall > Address**.
2 Select the internal interface.
3 Select New to add an address.
4 Enter the Address Name, IP Address, and NetMask for a single computer or for an entire subnetwork on an internal interface of the local VPN peer.
5 Select OK to save the source address.

To add a firewall policy

Add a policy that specifies the source and destination addresses and sets the service for the policy to the traffic type inside the L2TP VPN tunnel.

1 Go to **Firewall > Policy**.
2 Select the Ext->Int policy list.
3 Select New to add a policy.
4 Set Source to the group that matches the L2TP address range.
5 Set Destination to the address to which L2TP users can connect.
6 Set Service to match the traffic type inside the L2TP VPN tunnel.
For example, if L2TP users can access a web server, select HTTP.
7 Set Action to ACCEPT.
8 Select NAT if address translation is required.
You can also configure traffic shaping, logging, and antivirus and web filter settings for L2TP policies.
9 Select OK to save the firewall policy.

Configuring a Windows 2000 client for L2TP

Use the following procedure to configure a client computer running Windows 2000 so that it can connect to a FortiGate L2TP VPN.

To configure an L2TP dialup connection

1 Go to **Start > Settings > Network and Dial-up Connections**.
2 Double-click Make New Connection to start the Network Connection Wizard and select Next.
3 For Network Connection Type, select Connect to a private network through the Internet and select Next.
4 For Destination Address, enter the address of the FortiGate unit to connect to and select Next.
5 Set Connection Availability to Only for myself and select Next.
6 Select Finish.
7 In the Connect window, select Properties.

8 Select the Security tab.

9 Make sure that Require data encryption is selected.

Note: If a RADIUS server is used for authentication do not select Require data encryption. L2TP encryption is not supported for RADIUS server authentication.

10 Select the Networking tab.

11 Set VPN server type to Layer-2 Tunneling Protocol (L2TP).

12 Save the changes and continue with the following procedure.

To disable IPSec

1 Select the Networking tab.

2 Select Internet Protocol (TCP/IP) properties.

3 Double-click the Advanced tab.

4 Go to the Options tab and select IP security properties.

5 Make sure that Do not use IPSEC is selected.

6 Select OK and close the connection properties window.

Note: The default Windows 2000 L2TP traffic policy does not allow L2TP traffic without IPSec encryption. You can disable default behavior by editing the Windows 2000 Registry as described in the following steps. See the Microsoft documentation for editing the Windows Registry.

7 Use the registry editor (regedit) to locate the following key in the registry:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\
Parameters
```

8 Add the following registry value to this key:

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

9 Save the changes and restart the computer for the changes to take effect.

You must add the `ProhibitIpSec` registry value to each Windows 2000-based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the `ProhibitIpSec` registry value is set to 1, your Windows 2000-based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or active directory IPSec policy.

To connect to the L2TP VPN

1 Start the dialup connection that you configured in the previous procedure.

2 Enter your L2TP VPN User Name and Password.

3 Select Connect.

4 In the connect window, enter the User Name and Password that you use to connect to your dialup network connection.

This user name and password is not the same as your VPN user name and password.

Configuring a Windows XP client for L2TP

Use the following procedure to configure a client computer running Windows XP so that it can connect to a FortiGate L2TP VPN.

To configure an L2TP VPN dialup connection

1. Go to **Start > Settings**.
2. Select Network and Internet Connections.
3. Select Create a connection to the network of your workplace and select Next.
4. Select Virtual Private Network Connection and select Next.
5. Name the connection and select Next.
6. If the Public Network dialog box appears, choose the appropriate initial connection and select Next.
7. In the VPN Server Selection dialog, enter the IP address or host name of the FortiGate unit to connect to and select Next.
8. Select Finish.

To configure the VPN connection

1. Right-click the icon that you created.
2. Select **Properties > Security**.
3. Select Typical to configure typical settings.
4. Select Require data encryption.

Note: If a RADIUS server is used for authentication do not select Require data encryption. L2TP encryption is not supported for RADIUS server authentication.

5. Select Advanced to configure advanced settings.
6. Select Settings.
7. Select Challenge Handshake Authentication Protocol (CHAP).
8. Make sure that none of the other settings are selected.
9. Select the Networking tab.
10. Make sure that the following options are selected:
    - TCP/IP
    - QoS Packet Scheduler
11. Make sure that the following options are not selected:
    - File and Printer Sharing for Microsoft Networks
    - Client for Microsoft Networks

To disable IPSec

1. Select the Networking tab.
2. Select Internet Protocol (TCP/IP) properties.
3. Double-click the Advanced tab.

4 Go to the Options tab and select IP security properties.

5 Make sure that Do not use IPSEC is selected.

6 Select OK and close the connection properties window.

Note: The default Windows XP L2TP traffic policy does not allow L2TP traffic without IPSec encryption. You can disable default behavior by editing the Windows XP Registry as described in the following steps. See the Microsoft documentation for editing the Windows Registry.

7 Use the registry editor (regedit) to locate the following key in the registry:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\
Parameters
```

8 Add the following registry value to this key:

```
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1
```

9 Save the changes and restart the computer for the changes to take effect.

You must add the `ProhibitIpSec` registry value to each Windows XP-based endpoint computer of an L2TP or IPSec connection to prevent the automatic filter for L2TP and IPSec traffic from being created. When the `ProhibitIpSec` registry value is set to 1, your Windows XP-based computer does not create the automatic filter that uses CA authentication. Instead, it checks for a local or active directory IPSec policy.

To connect to the L2TP VPN

1 Connect to your ISP.

2 Start the VPN connection that you configured in the previous procedure.

3 Enter your L2TP VPN User Name and Password.

4 Select Connect.

5 In the connect window, enter the User Name and Password that you use to connect to your dialup network connection.

This user name and password is not the same as your VPN user name and password.

Network Intrusion Detection System (NIDS)

The FortiGate NIDS is a real-time network intrusion detection sensor that uses attack signature definitions to both detect and prevent a wide variety of suspicious network traffic and direct network-based attacks. Also, whenever an attack occurs, the FortiGate NIDS can record the event in a log and send an alert email to the system administrator.

This chapter describes:

Detecting attacks

The NIDS Detection module detects a wide variety of suspicious network traffic and network-based attacks. Use the following procedures to configure the general NIDS settings and the NIDS Detection module Signature List.

For the general NIDS settings, you must select which interfaces you want to be monitored for network-based attacks. You also need to decide whether to enable checksum verification. Checksum verification tests the integrity of packets received at the monitored interfaces.

This section describes:

Selecting the interfaces to monitor

To select the interfaces to monitor for attacks

1 Go to **NIDS > Detection > General**.

2 Select the interfaces to monitor for network attacks.
You can select one or more interfaces.

3 Select Apply.

Disabling monitoring interfaces

To disable monitoring interfaces for attacks

1 Go to **NIDS > Detection > General**.

2 Clear the check box for all the interfaces that you do not want monitored.

3 Select Apply.

Configuring checksum verification

Checksum verification tests the files that pass through the FortiGate unit to make sure that they have not been changed in transit. The NIDS can run checksum verification on IP, TCP, UDP, and ICMP traffic. For maximum detection, you can turn on checksum verification for all types of traffic. However, if the FortiGate unit does not need to run checksum verification, you can turn it off for some or all types of traffic to improve system performance. For example, you might not need to run checksum verification if the FortiGate unit is installed behind a router that also does checksum verification.

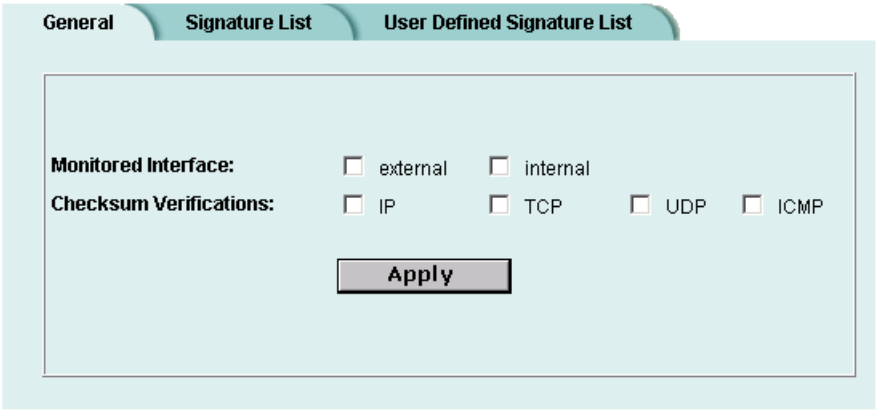
To configure checksum verification

1 Go to **NIDS > Detection > General**.

2 Select the type of traffic that you want to run Checksum Verifications on.

3 Select Apply.

Figure 31: Example NIDS detection configuration



Viewing the signature list

You can display the current list of NIDS signature groups and the members of a signature group.

To view the signature list

1 Go to **NIDS > Detection > Signature List**.

2 View the names and action status of the signature groups in the list.
The NIDS detects attacks listed in all the signature groups that have check marks in the Enable column.

Note: The user-defined signature group is the last item in the signature list. See "Adding user-defined signatures" on page 218.

3 Select View Details  .to display the members of a signature group.
The Signature Group Members list displays the attack ID, Rule Name, and Revision number for each group member.

Viewing attack descriptions

Fortinet provides online information for all NIDS attacks. You can view the FortiResponse Attack Analysis web page for an attack listed on the signature list.

To view attack descriptions

1 Go to **NIDS > Detection > Signature List**.

2 Select View Details  .to display the members of a signature group.

3 Select a signature and copy its attack ID.

4 Open a web browser and enter the following URL:
`http://www.fortinet.com/ids/ID<attack-ID>`
Make sure that you include the attack ID.
For example, to view the Fortinet Attack Analysis web page for the `ssh CRC32 overflow /bin/sh` attack (ID 101646338), use the following URL:
`http://www.fortinet.com/ids/ID101646338`

Note: Each attack log message includes a URL that links directly to the FortiResponse Attack Analysis web page for that attack. This URL is available in the Attack Log messages and Alert email messages. For information about log message content and formats, and about log locations, see the *FortiGate Logging and Message Reference Guide*. For information about logging attack messages, see "Logging attacks" on page 222.

Figure 32: Example signature group members list

exploit		
ID	**Rule Name**	**Revision**
101646337	gobbles SSH exploit attempt	16
101646338	ssh CRC32 overflow /bin/sh	16
101646339	ssh CRC32 overflow NOOP	16
101646340	ssh CRC32 overflow	16
101646341	x86 linux samba overflow	16
101646342	Solaris x86 nlps overflow attempt	16
101646343	nlps x86 solaris overflow	16
101646344	LPRng overflow	16
101646345	redhat 7.0 lprd overflow	16

Disabling NIDS attack signatures

By default, all NIDS attack signatures are enabled. You can use the NIDS signature list to disable detection of some attacks. Disabling unnecessary NIDS attack signatures can improve system performance and reduce the number of IDS log messages and alert emails that the NIDS generates. For example, the NIDS detects a large number of web server attacks. If you do not provide access to a web server behind your firewall, you might want to disable all web server attack signatures.

Note: To save your NIDS attack signature settings, Fortinet recommends that you back up your FortiGate configuration before you update the firmware and restore the saved configuration after the update.

To disable NIDS attack signatures

1. Go to **NIDS > Detection > Signature List**.
2. Scroll through the signature list to find the signature group that you want to disable.
   Attack ID numbers and rule names in attack log messages and alert email match those in the signature group members list. You can scroll through a signature group members list to locate specific attack signatures by ID number and name.
3. Clear the Enable check box.
4. Select OK.
5. Repeat steps 2 to 4 for each NIDS attack signature group that you want to disable.
   Select Check All  to enable all NIDS attack signature groups in the signature list.
   Select Uncheck All  to disable all NIDS attack signature groups in the signature list.

Adding user-defined signatures

You can create a user-defined signature list in a text file and upload it from the management computer to the FortiGate unit.

Note: You cannot upload individual signatures. You must include, in a single text file, all the user-defined signatures that you want to upload. The file can contain one or more signatures.

For information about how to write user-defined signatures, see the *FortiGate NIDS Guide*.

To add user-defined signatures

1 Go to **NIDS > Detection > User Defined Signature List**.

2 Select Upload .

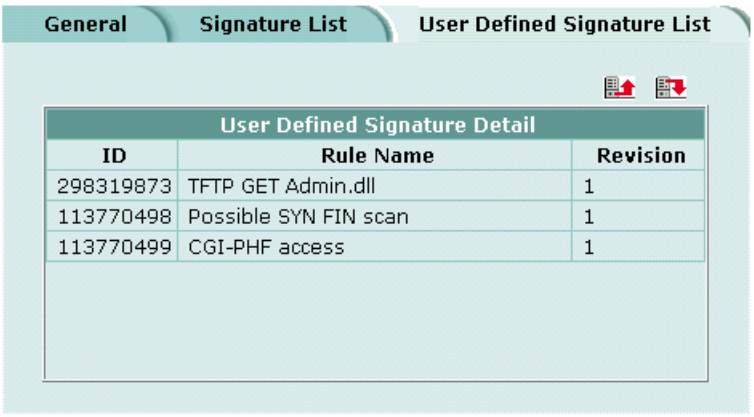
Caution: Uploading the user-defined signature list overwrites the existing file.

3 Type the path and filename of the text file for the user-defined signature list or select Browse and locate the file.

4 Select OK to upload the text file for the user-defined signature list.

5 Select Return to display the uploaded user-defined signature list.

Figure 33: Example user-defined signature list



Downloading the user-defined signature list

You can back up the user-defined signature list by downloading it to a text file on the management computer.

Note: You cannot download individual signatures. You must download the entire user-defined signature list.

To download the user-defined signature list

1 Go to **NIDS > Detection > User Defined Signature List**.

2 Select Download.

The FortiGate unit downloads the user-defined signature list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

Preventing attacks

NIDS attack prevention protects the FortiGate unit and the networks connected to it from common TCP, ICMP, UDP, and IP attacks. You can enable NIDS attack prevention to prevent a set of default attacks with default threshold values. You can also enable or disable and set the threshold values for individual attack prevention signatures.

Note: After the FortiGate unit reboots, NIDS attack prevention and synflood prevention are always disabled.

Enabling NIDS attack prevention

To enable NIDS attack prevention

1. Go to **NIDS > Prevention**.
2. Select the Enable Prevention check box, in the top left corner.

Enabling NIDS attack prevention signatures

The NIDS Prevention module contains signatures that are designed to protect your network against attacks. Some signatures are enabled by default, others must be enabled. For a complete list of NIDS Prevention signatures and descriptions, see the *FortiGate NIDS Guide*.

To enable attack prevention signatures

1. Go to **NIDS > Prevention**.
2. Select the Enable check box beside each signature that you want to enable.
3. Select Check All to enable all signatures in the NIDS attack prevention signature list.
4. Select Uncheck All to disable all signatures in the NIDS attack prevention signature list.
5. Select Reset to Default Values to enable only the default NIDS attack prevention signatures and return to the default threshold values.

Setting signature threshold values

You can change the default threshold values for the NIDS Prevention signatures listed in Table 20. The threshold depends on the type of attack. For flooding attacks, the threshold is the maximum number of packets received per second. For overflow attacks, the threshold is the buffer size for the command. For large ICMP attacks, the threshold is the ICMP packet size limit to pass through.

For example, setting the icmpflood signature threshold to 500 allows 500 echo requests from a source address, to which the system sends echo replies. The FortiGate unit drops any requests over the threshold of 500.

If you enter a threshold value of 0 or a number out of the allowable range, the FortiGate unit uses the default value.

Table 20: NIDS Prevention signatures with threshold values

Signature abbreviation	Threshold value units	Default threshold value	Minimum threshold value	Maximum threshold value
synflood	Threshold: Maximum number of SYN segments received per second.	2048	1	1000000
	Queue Size: Maximum proxied connections.	4096	100	1000000
	Timeout: Number of seconds for the SYN cookie to keep a proxied connection alive.	15	1	3600
portscan	Maximum number of SYN segments received per second	512	1	1000000
srcsession	Total number of TCP sessions initiated from the same source	2048	1	1000000
ftpovfl	Maximum buffer size for an FTP command (bytes)	256	32	1408
smtpovfl	Maximum buffer size for an SMTP command (bytes)	512	32	1408
pop3ovfl	Maximum buffer size for a POP3 command (bytes)	512	32	1408
udpflood	Maximum number of UDP packets received from the same source or sent to the same destination per second	2048	1	1000000
udpsrcsession	Total number of UDP sessions initiated from the same source	2048	1	1000000
icmpflood	Maximum number of ICMP packets received from the same source or sent to the same destination per second	256	1	1000000
icmpsrcsession	Total number of ICMP sessions initiated from the same source	128	1	1000000
icmpsweep	Maximum number of ICMP packets received from the same source per second	128	1	1000000
icmplarge	Maximum ICMP packet size (bytes)	32000	64	64000

To set Prevention signature threshold values

1 Go to **NIDS > Prevention**.
2 Select Modify beside the signature for which you want to set the Threshold value.
Signatures that do not have threshold values do not have Modify icons.
3 Type the Threshold value.
4 Select the Enable check box.
5 Select OK.

Logging attacks

Whenever the NIDS detects or prevents an attack, it generates an attack message. You can configure the system to add the message to the attack log.

- Logging attack messages to the attack log
- Reducing the number of NIDS attack log and email messages

Logging attack messages to the attack log

To log attack messages to the attack log

1 Go to **Log&Report > Log Setting**.
2 Select Config Policy for the log locations you have set.
3 Select Attack Log.
4 Select Attack Detection and Attack Prevention.
5 Select OK.

Note: For information about log message content and formats, and about log locations, see the *FortiGate Logging and Message Reference Guide*.

Reducing the number of NIDS attack log and email messages

Intrusion attempts might generate an excessive number of attack messages. Based on the frequency that messages are generated, the FortiGate unit automatically deletes duplicates. If you still receive an excessive number of unnecessary messages, you can manually disable message generation for unneeded signature groups.

Automatic message reduction

The attack log and alert email messages that the NIDS produces include the ID number and name of the attack that generated the message. The attack ID number and name in the message are identical to the ID number and rule name that appear on the NIDS Signature Group Members list.

The FortiGate unit uses an alert email queue in which each new message is compared with the previous messages. If the new message is not a duplicate, the FortiGate unit sends it immediately and puts a copy in the queue. If the new message is a duplicate, the FortiGate unit deletes it and increases an internal counter for the number of message copies in the queue.

The FortiGate unit holds duplicate alert email messages for 60 seconds. If a duplicate message has been in the queue for more than 60 seconds, the FortiGate unit deletes the message and increases the copy number. If the copy number is greater than 1, the FortiGate unit sends a summary email that includes “Repeated *x* times” in the subject header, the statement “The following email has been repeated *x* times in the last *y* seconds”, and the original message.

Manual message reduction

If you want to reduce the number of alerts that the NIDS generates, you can review the content of attack log messages and alert email. If a large number of the alerts are nuisance alerts (for example, web attacks when you are not running a web server), you can disable the signature group for that attack type. Use the ID number in the attack log or alert email to locate the attack in the signature group list. See “Disabling NIDS attack signatures” on page 218.

Antivirus protection

You can enable antivirus protection in firewall policies. You can select a content profile that controls how the antivirus protection behaves. Content profiles control the type of traffic protected (HTTP, FTP, IMAP, POP3, SMTP), the type of antivirus protection and the treatment of fragmented email and oversized files or email.

This chapter describes:

General configuration steps

Configuring antivirus protection involves the following general steps.

1. Select antivirus protection options in a new or existing content profile. See “Adding content profiles” on page 167.
2. Select the Anti-Virus & Web filter option in firewall policies that allow web (HTTP), FTP, and email (IMAP, POP3, and SMTP) connections through the FortiGate unit. Select a content profile that provides the antivirus protection options that you want to apply to a policy. See “Adding content profiles to policies” on page 169.
3. Configure antivirus protection settings to control how the FortiGate unit applies antivirus protection to the web, FTP, and email traffic allowed by policies. See:
   - “Antivirus scanning” on page 226,
   - “File blocking” on page 227,
   - “Blocking oversized files and emails” on page 228,
   - “Exempting fragmented email from blocking” on page 228.
4. Configure the messages that users receive when the FortiGate unit blocks or deletes an infected file. See “Replacement messages” on page 133.
5. Configure the FortiGate unit to send an alert email when it blocks or deletes an infected file. See “Configuring alert email” in the *Logging and Message Reference Guide.*

Note: For information about receiving virus log messages, see “Configuring logging”, and for information about log message content and format, see “Virus log messages” in the *Logging Configuration and Reference Guide*

Antivirus scanning

Virus scanning intercepts most files (including files compressed with up to 12 layers of compression using zip, rar, gzip, tar, upx, and OLE) in the content streams for which you enable antivirus protection. Each file is tested to determine the file type and the most effective method of scanning the file for viruses. For example, binary files are scanned using binary virus scanning and Microsoft Office files containing macros are scanned for macro viruses.

FortiGate virus scanning does not scan the following file types:

- cdimage
- floppy image
- .ace
- .bzip2
- .Tar+Gzip+Bzip2

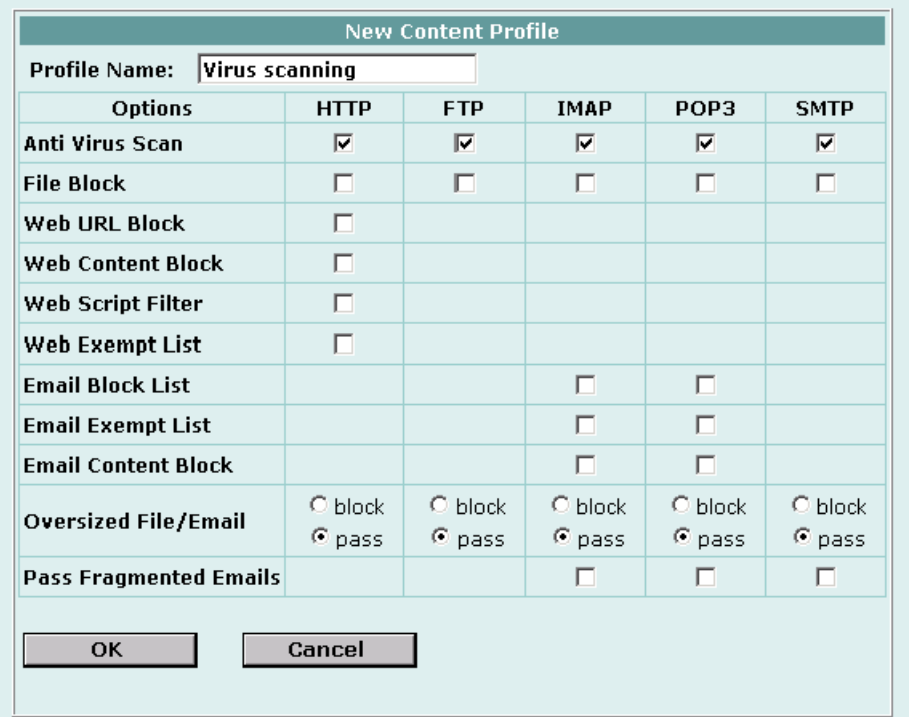
If a file is found to contain a virus, the FortiGate unit removes the file from the content stream and replaces it with a replacement message.

To scan FortiGate firewall traffic for viruses

1 Select antivirus scanning in a content profile.
For information about content profiles, see "Adding content profiles" on page 167.

2 Add this content profile to firewall policies to apply virus scanning to the traffic controlled by the firewall policy.
See "Adding content profiles to policies" on page 169.

Figure 34: Example content profile for virus scanning



File blocking

Enable file blocking to remove all files that are a potential threat and to provide the best protection from active computer virus attacks. Blocking files is the only protection from a virus that is so new that antivirus scanning cannot detect it. You would not normally operate the FortiGate unit with blocking enabled. However, it is available for extremely high-risk situations in which there is no other way to prevent viruses from entering your network.

File blocking deletes all files that match a list of enabled file patterns. The FortiGate unit replaces the file with an alert message that is forwarded to the user. The FortiGate unit also writes a message to the virus log and sends an alert email if it is configured to do so.

Note: If both blocking and scanning are enabled, the FortiGate unit blocks files that match enabled file patterns and does not scan these files for viruses.

By default, when blocking is enabled, the FortiGate unit blocks the following 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)

Blocking files in firewall traffic

Use content profiles to apply file blocking to HTTP, FTP, POP3, IMAP, and SMTP traffic controlled by firewall policies.

To block files in firewall traffic

1. Select file blocking in a content profile.
   See “Adding content profiles” on page 167.
2. Add this content profile to firewall policies to apply content blocking to the traffic controlled by the firewall policy.
   See “Adding content profiles to policies” on page 169.

Adding file patterns to block

To add file patterns to block

1. Go to **Anti-Virus > File Block**.
2. Select New.

3 Type the new pattern in the File Pattern field.
You can use an asterisk (*) to represent any characters and a question mark (?) to represent any single character. For example, *.dot blocks Microsoft Word template files and *.do? blocks both Microsoft Word template files and document files.

4 Select the check box beside the traffic protocols for which you want to enable blocking of this file pattern.

5 Select OK.

Blocking oversized files and emails

You can configure the FortiGate unit to buffer 1 to 15 percent of available memory to store oversized files and email. The FortiGate unit then blocks a file or email that exceeds this limit instead of bypassing antivirus scanning and sending the file or email directly to the server or receiver. The FortiGate unit sends a replacement message for an oversized file or email attachment to the HTTP or email proxy client.

Configuring limits for oversized files and email

To configure limits for oversized files and email

1 Go to **Anti-Virus > Config > Config**.

2 Type the size limit, in MB.

3 Select Apply.

Exempting fragmented email from blocking

A fragmented email is a large email message that has been split into smaller messages that are sent individually and recombined when they are received. By default, when antivirus protection is enabled, the FortiGate unit blocks fragmented emails and replaces them with an email block message that is forwarded to the receiver. It is recommended that you disable the fragmenting of email messages in the client email software.

To exempt fragmented emails from automatic antivirus blocking

Caution: The FortiGate unit cannot scan fragmented emails for viruses or use file pattern blocking to remove files from these email messages.

1 Enable Pass Fragmented Emails for IMAP, POP3, and SMTP traffic in a content profile.

2 Select Anti-Virus & Web filter in a firewall policy. For example, to pass fragmented emails that internal users send to the external network, select an internal to external policy.

3 Select a content profile that has Pass Fragmented Emails enabled for the traffic that you want the FortiGate unit to scan.

Viewing the virus list

You can view the names of the viruses and worms in the current virus definition list.

To view the virus list

1. Go to **Anti-Virus > Config > Virus List**.
2. Scroll through the virus and worm list to view the names of all viruses and worms in the list.

Web filtering

When you enable Anti-Virus & Web filter in a firewall policy, you select a content profile that controls how web filtering behaves for HTTP traffic. Content profiles control the following types of content filtering:

- blocking unwanted URLs,
- blocking unwanted content,
- removing scripts from web pages,
- exempting URLs from blocking.

You can also use the Cerberian URL filtering to block unwanted URLs. For more information, see "Configuring Cerberian URL filtering" on page 238.

This chapter describes:

General configuration steps

Configuring web filtering involves the following general steps:

1. Select web filtering options in a new or existing content profile. See "Adding content profiles" on page 167.
2. Select the Anti-Virus & Web filter option in firewall policies that allow HTTP connections through the FortiGate unit.
   - Select a content profile that provides the web filtering options that you want to apply to a policy. See "Adding content profiles to policies" on page 169.
3. Configure web filtering settings to control how the FortiGate unit applies web filtering to the HTTP traffic allowed by policies. See:
   - "URL blocking" on page 235,
   - "Configuring Cerberian URL filtering" on page 238,
   - "Content blocking" on page 232,
   - "Script filtering" on page 240,
   - "Exempt URL list" on page 241.

4 Configure the messages that users receive when the FortiGate unit blocks unwanted content or unwanted URLs. See “Replacement messages” on page 133.

5 Configure the FortiGate unit to record log messages when it blocks unwanted content or unwanted URLs. See “Recording logs” on page 251.

6 Configure the FortiGate unit to send an alert email when it blocks unwanted content or unwanted URLs. See “Configuring alert email” on page 257.

Content blocking

When the FortiGate unit blocks a web page, the user who requested the blocked page receives a block message and the FortiGate unit writes a message to the web filtering log.

You can add banned words to the list in many languages using Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean character sets.

- Adding words and phrases to the Banned Word list
- Clearing the Banned Word list
- Backing up the Banned Word list
- Restoring the Banned Word list

Adding words and phrases to the Banned Word list

1 Go to **Web Filter > Content Block**.

2 Select New to add a word or phrase to the Banned Word list.

3 Choose a language or character set for the banned word or phrase.

You can choose Western, Chinese Simplified, Chinese Traditional, Japanese, or Korean.

Your computer and web browser must be configured to enter characters in the character set that you choose.

4 Type a banned word or phrase.

If you type a single word (for example, `banned`), the FortiGate unit blocks all web pages that contain that word.

If you type a phrase (for example, `banned phrase`), the FortiGate unit blocks web pages that contain both words. When this phrase appears on the banned word list, the FortiGate unit inserts plus signs (+) in place of spaces (for example, `banned+phrase`).

If you type a phrase in quotes (for example, `"banned word"`), the FortiGate unit blocks all web pages in which the words are found together as a phrase.

Content filtering is not case-sensitive. You cannot include special characters in banned words.

5 To enable the banned word, ensure that the Enable checkbox is selected.

6 Select OK.

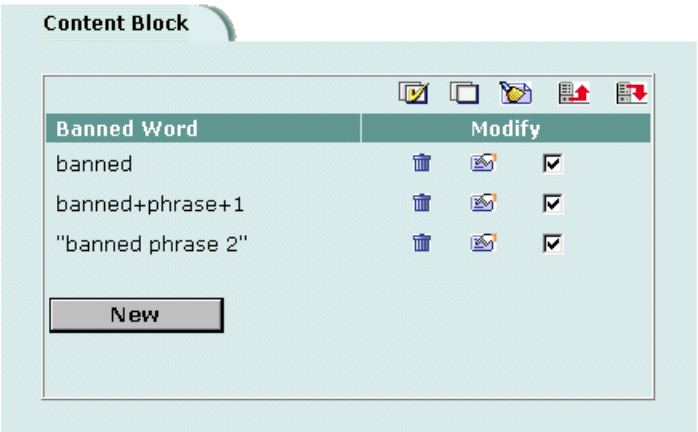
The word or phrase is added to the Banned Word list.

You can enable all the words on the banned word list by selecting Check All  .

You can disable all the words on the banned word list by selecting Uncheck All  .

Note: Banned Word must be selected in the content profile for web pages containing banned words to be blocked.

Figure 35: Example banned word list



Clearing the Banned Word list

1 Go to **Web Filter > Content Block**.

2 Select Clear List to remove all banned words and phrases from the banned word list.

Backing up the Banned Word list

You can back up the banned word list by downloading it to a text file on the management computer.

To back up the banned word list

1 Go to **Web Filter > Content Block**.

2 Select Backup Banned Word List.
The FortiGate unit downloads the list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

Restoring the Banned Word list

You can create a Banned Word list in a text editor and then upload the text file to the FortiGate unit. Add one banned word or phrase to each line of the text file. The word or phrase should be followed by two parameters separated by spaces. The first parameter specifies the status of the entry. The second parameter specifies the language of the entry.

Table 21: Banned Word list configuration parameters

Parameter	Setting	Description
Status	0	Disabled
	1	Enabled
Language	0	ASCII
	1	Simplified Chinese
	2	Traditional Chinese
	3	Japanese
	4	Korean

Figure 36: Example Banned Word List text file

```
banned 1 0
banned+phrase+1 1 3
"banned+phrase+2" 1 1
```

Note: All changes made to the banned word list using the web-based manager are lost when you upload a new list. However, you can download your current banned word list, add more items to it using a text editor, and then upload the edited list to the FortiGate unit.

To restore the banned word list

1. Go to **Web Filter > Content Block**.
2. Select Restore Banned Word List .
3. Type the path and filename of the banned word list text file, or select Browse and locate the file.
4. Select OK to upload the file to the FortiGate unit.
5. Select Return to display the updated Banned Word List.
6. You can continue to maintain the Banned Word List by making changes to the text file and uploading it again as necessary.

Note: Banned Word must be selected in the content profile for web pages containing banned words to be blocked.

URL blocking

You can block the unwanted web URLs using FortiGate Web URL blocking, FortiGate Web pattern blocking, and Cerberian web filtering.

- Configuring FortiGate Web URL blocking
- Configuring FortiGate Web pattern blocking
- Configuring Cerberian URL filtering

Configuring FortiGate Web URL blocking

You can configure FortiGate Web URL blocking to block all pages on a website by adding the top-level URL or IP address. You can also block individual pages on a website by including the full path and filename of the web page to block.

- Adding URLs to the Web URL block list
- Clearing the Web URL block list
- Downloading the Web URL block list
- Uploading a URL block list

Adding URLs to the Web URL block list

1 Go to **Web Filter > Web URL Block**.

2 Select New to add a URL to the Web URL block list.

3 Type the URL the you want to block.

Type a top-level URL or IP address to block access to all pages on a website. For example, `www.badsite.com` or `122.133.144.155` blocks access to all pages at this website.

Type a top-level URL followed by the path and filename to block access to a single page on a website. For example, `www.badsite.com/news.html` or `122.133.144.155/news.html` blocks the news page on this website.

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.

Note: Do not include `http://` in the URL that you want to block.

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 “Configuring FortiGate Web pattern blocking” on page 237.

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.

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.

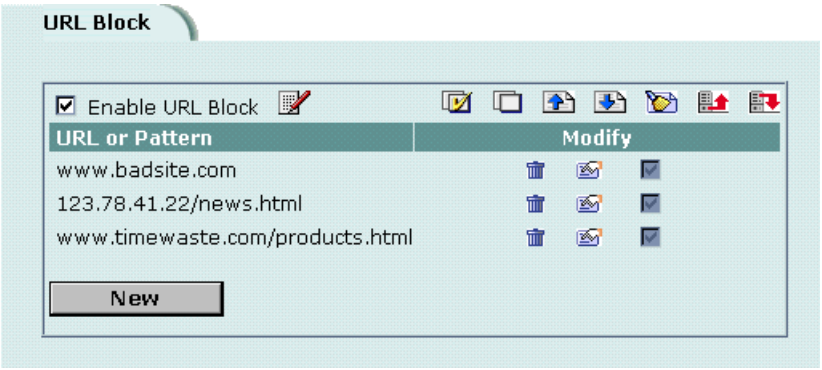
4 Ensure that the Enable checkbox has been selected and then select OK.

5 Select OK to add the URL to the Web URL block list.
You can enter multiple URLs and then select Check All to enable all items in the Web URL block list.
You can disable all of the URLs on the list by selecting Uncheck All .
Each page of the Web URL block list displays 100 URLs.

6 Use Page Up and Page Down to navigate through the Web URL block list.

Note: You must select the Web URL Block option in the content profile to enable the URL blocking.

Figure 37: Example URL block list



Clearing the Web URL block list

1 Go to **Web Filter > Web URL Block**.

2 Select Clear URL Block List to remove all URLs and patterns from the Web URL block list.

Downloading the Web URL block list

You can back up the Web URL block list by downloading it to a text file on the management computer.

To download a Web URL block list

1 Go to **Web Filter > Web URL Block**.

2 Select Download URL Block List .
The FortiGate unit downloads the list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

Uploading a URL block list

You can create a URL block list in a text editor and then upload the text file to the FortiGate unit. Add one URL or pattern to each line of the text file. You can follow the item with a space and then a 1 to enable or a zero (0) to disable the URL. If you do not add this information to the text file, the FortiGate unit automatically enables all URLs and patterns that are followed by a 1 or no number when you upload the text file.

Figure 38: Example URL block list text file

```
www.badsite.com/index 1
www.badsite.com/products 1
182.63.44.67/index 1
```

You can either create the URL block list or add a URL list created by a third-party URL block or blacklist service. For example, you can download the squidGuard blacklists available at http://www.squidguard.org/blacklist/ as a starting point for creating a URL block list. Three times per week, the squidGuard robot searches the web for new URLs to add to the blacklists. You can upload the squidGuard blacklists to the FortiGate unit as a text file, with only minimal editing to remove comments at the top of each list and to combine the lists that you want into a single file.

Note: All changes made to the URL block list using the web-based manager are lost when you upload a new list. However, you can download your current URL block list, add more items to it using a text editor, and then upload the edited list to the FortiGate unit.

To upload a URL block list

1. In a text editor, create the list of URLs and patterns that you want to block.
2. Using the web-based manager, go to **Web Filter > Web URL Block**.
3. Select Upload URL Block List .
4. Type the path and filename of the URL block list text file, or select Browse and locate the file.
5. Select OK to upload the file to the FortiGate unit.
6. Select Return to display the updated Web URL block list.
   Each page of the Web URL block list displays 100 URLs.
7. Use Page Down and Page Up to navigate through the Web URL block list.
8. You can continue to maintain the Web URL block list by making changes to the text file and uploading it again.

Configuring FortiGate Web pattern blocking

You can configure FortiGate web pattern blocking to block web pages that match a URL pattern. Create URL patterns using regular expressions (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.

To add patterns to the Web pattern block list

1. Go to **Web Filter > URL Block > Web Pattern Block**.
2. Select New to add an item to the Web pattern block list.
3. Type the web pattern that you want to block.
   You can use standard regular expressions for web patterns.

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.

4 Select Enable to block the pattern.

5 Select OK to add the pattern to the Web pattern block list.

Note: You must select the Web URL Block option in the content profile to enable the URL blocking.

Configuring Cerberian URL filtering

The FortiGate unit supports Cerberian URL filtering. For information about Cerberian URL filtering, see www.cerberian.com.

If you have purchased the Cerberian web filtering functionality with your FortiGate unit, use the following configuration procedures to configure FortiGate support for Cerberian web filtering.

- Installing a Cerberian license key
- Adding a Cerberian user
- Configuring Cerberian web filter
- Enabling Cerberian URL filtering

Installing a Cerberian license key

Before you can use the Cerberian web filter, you must install a license key. The license key determines the number of end users allowed to use Cerberian web filtering through the FortiGate unit.

To install a Cerberian licence key

1 Go to **Web Filter > URL Block**.

2 Select Cerberian URL Filtering.

3 Enter the license number.

4 Select Apply.

Adding a Cerberian user

The Cerberian web policies can be applied only to user groups. You can add users on the FortiGate unit and then add the users to user groups on the Cerberian administration web site.

When the end user tries to access a URL, the FortiGate unit checks whether the user's IP address is in the IP address list on the FortiGate unit. If the user's IP address is in the list, the request is sent to the Cerberian server. Otherwise, an error message is sent to the user saying that the user does not have authorized access to the Cerberian web filter.

To add a Cerberian user

1 Go to **Web Filter > URL Block**.

2 Select Cerberian URL Filtering.

3 Select New.

4 Enter the IP address and netmask of the user computers.
You can enter the IP address of a single user. For example, 192.168.100.19 255.255.255.255. You can also enter a subnet of a group of users. For example, 192.168.100.0 255.255.255.0.

5 Enter an alias for the user.
The alias is used as the user name when you add the user to a user group on the Cerberian server. If you do not enter an alias, the user's IP is used and added to the default group on the Cerberian server.

6 Select OK.

Configuring Cerberian web filter

After you add the Cerberian web filter users on the FortiGate unit, you can add these users to the user groups on the Cerberian web filter server. Then you can create policies and apply these policies to the user groups.

About the default group and policy

There is a default user group, which is associated with a default policy, that exists on the Cerberian web filter server.

You can add users to the default group and apply any policies to the group.

Use the default group to add:

- All the users who are not assigned alias names on the FortiGate unit.
- All the users who are not assigned to other user groups.

The Cerberian web filter groups URLs into 53 categories. The default policy blocks the URLs of 12 categories. You can modify the default policy and apply it to any user groups.

To configure Cerberian web filtering

1 Add the user name, which is the alias you added on the FortiGate unit, to a user group on the Cerberian server.
Web policies can be applied only to user groups. If you did not enter an alias for a user's IP address on the FortiGate unit, the user's IP address is automatically added to the default Cerberian group.

2 Create policies by selecting the web categories that you want to block.

3 Apply the policy to a user group that contains the user.
For detailed procedures, see the online help on the Cerberian Web Filter web page.

Enabling Cerberian URL filtering

After you add the Cerberian users and groups and configure the Cerberian web filter, you can enable Cerberian URL filtering.

To enable cerberian URL filtering

1 Go to **Web Filter > URL Block > Cerberian URL Filtering**.

2 Select the Cerberian URL Filtering option.

3 Go to **Firewall > Content Profile**.
4 Create a new or select an existing content profile and enable Web URL Block.
5 Go to **Firewall > Policy**.
6 Create a new or select an existing policy.
7 Select Anti-Virus & Web filter.
8 Select the content profile from the Content Profile list.
9 Select OK.

Script filtering

You can configure the FortiGate unit to remove Java applets, cookies, and ActiveX scripts from the HTML web pages.

Note: Blocking any of these items might prevent some web pages from working properly.

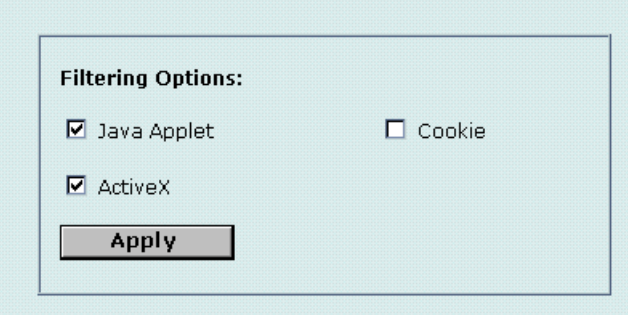
Enabling script filtering

1 Go to **Firewall > Content Profile**.
2 Select the content profile for which you want to enable script filtering.
3 Select Script Filter.
4 Select OK.

Selecting script filter options

1 Go to **Web Filter > Script Filter.**
2 Select the script filter options that you want to enable.
You can block Java applets, cookies, and ActiveX.
3 Select Apply.

Figure 39: Example script filter settings to block Java applets and ActiveX



Exempt URL list

Add URLs to the exempt URL list to allow legitimate traffic that might otherwise be blocked by content or URL blocking. For example, if content blocking is set to block pornography-related words and a reputable website runs a story on pornography, web pages from the reputable website are blocked. Adding the address of the reputable website to the exempt URL list allows the content of the website to bypass content blocking.

Note: Content downloaded from exempt web pages is not blocked or scanned by antivirus protection.

Adding URLs to the URL Exempt list

1. Go to **Web Filter > URL Exempt**.
2. Select New to add an item to the URL Exempt list.
3. Type the URL to exempt.

   Type a complete URL, including path and filename, to exempt access to a page on a website. For example, `www.goodsite.com/index.html` exempts access to the main page of this example website. You can also add IP addresses; for example, `122.63.44.67/index.html` exempts access to the main web page at this address. Do not include `http://` in the URL to exempt.

   Exempting a top-level URL, such as `www.goodsite.com`, exempts all requested subpages (for example, `www.goodsite.com/badpage`) from all content and URL filtering rules.

Note: Exempting a top-level URL does not exempt pages such as `mail.goodsite.com` from all content and URL filtering rules unless `goodsite.com` (without the `www`) is added to the exempt URL list.

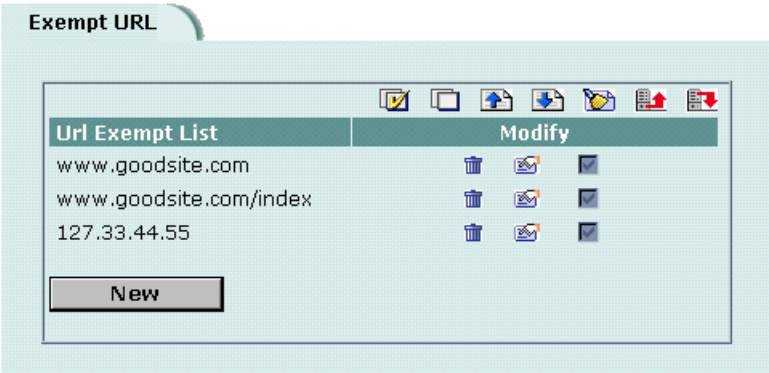
4. Ensure that the Enable checkbox has been selected.
5. Select OK to add the URL to the exempt URL list.

   You can enter multiple URLs and then select Check All  to activate all items in the exempt URL list.

   You can disable all the URLs in the list by selecting Uncheck All  .

   Each page of the exempt URL list displays 100 URLs.
6. Use Page Down  and Page Up  to navigate the exempt URL list.

Figure 40: Example URL Exempt list



Downloading the URL Exempt List

You can back up the URL Exempt List by downloading it to a text file on the management computer.

1 Go to **Web Filter > URL Exempt**.

2 Select Download URL Exempt List .

The FortiGate unit downloads the list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

Uploading a URL Exempt List

You can create a URL Exempt list in a text editor and then upload the text file to the FortiGate unit. Add one URL or pattern to each line of the text file. The word or phrase should be followed by a parameter specifying the status of the entry. If you do not add this information to the text file, the FortiGate unit automatically enables all URLs and patterns that are followed with a 1 or no number when you upload the text file.

Table 22: URL Exempt list configuration parameters

Parameter	Setting	Description
Status	0	Disabled
	1	Enabled

Figure 41: Example URL Exempt list text file

```
www.goodsite.com 1
www.goodsite.com/index 1
127.33.44.55 1
```

Note: All changes made to the URL block list using the web-based manager are lost when you upload a new list. However, you can download your current URL block list, add more items to it using a text editor, and then upload the edited list to the FortiGate unit.

1 In a text editor, create the list of URLs to exempt.

2 Using the web-based manager, go to **Web Filter > URL Exempt**.

3 Select Upload URL Exempt List  .

4 Type the path and filename of your URL Exempt List text file, or select Browse and locate the file.

5 Select OK to upload the file to the FortiGate unit.

6 Select Return to display the updated URL Exempt List.

7 You can continue to maintain the URL Exempt List by making changes to the text file and uploading it again as necessary.

Email filter

Email filtering is enabled in firewall policies. When you enable Anti-Virus & Web filter in a firewall policy, you select a content profile that controls how email filtering behaves for email (IMAP and POP3) traffic. Content profiles control the following types of protection to identify unwanted email:

- filtering unwanted sender address patterns,
- filtering unwanted content,
- exempting sender address patterns from blocking.

This chapter describes:

General configuration steps

Configuring email filtering involves the following general steps:

1. Select email filter options in a new or existing content profile. See “Adding content profiles” on page 167.
2. Select the Anti-Virus & Web filter option in firewall policies that allow IMAP and POP3 connections through the FortiGate unit. Select a content profile that provides the email filtering options that you want to apply to a policy. See “Adding content profiles to policies” on page 169.
3. Add a subject tag to the unwanted email so that receivers can use their mail client software to filter messages based on the tag. See “Adding a subject tag” on page 250.

Note: For information about receiving email filter log messages, see “Configuring logging” in the *Logging Configuration and Reference Guide*. For information about email filter log message categories and formats, see “Log messages” in the *FortiGate Logging Configuration and Reference Guide.*

Email banned word list

When the FortiGate unit detects an email that contains a word or phrase in the banned word list, the FortiGate unit adds a tag to the subject line of the email and writes a message to the event log. Receivers can then use their mail client software to filter messages based on the subject tag.

You can add banned words to the list in many languages using Western, Simplified Chinese, Traditional Chinese, Japanese, or Korean character sets.

Adding words and phrases to the email banned word list

To add a word or phrase to the banned word list

1 Go to **Email Filter > Content Block**.

2 Select New.

3 Type a banned word or phrase.

- If you type a single word (for example, `banned`), the FortiGate unit tags all IMAP and POP3 email that contains that word.
- If you type a phrase (for example, `banned phrase`), the FortiGate unit tags email that contains both words. When this phrase appears on the banned word list, the FortiGate unit inserts plus signs (+) in place of spaces (for example, `banned+phrase`).
- If you type a phrase in quotes (for example, `"banned word"`), the FortiGate unit tags all email in which the words are found together as a phrase.

Content filtering is not case-sensitive. You cannot include special characters in banned words.

1 Select the Language for the banned word or phrase.

You can choose Western, Chinese Simplified, Chinese Traditional, Japanese, or Korean.

Your computer and web browser must be configured to enter characters in the language that you select.

2 Select OK.

The word or phrase is added to the banned word list.

Note: Email Content Block must be selected in the content profile for IMAP or POP3 email containing banned words to be tagged.

Downloading the email banned word list

You can back up the banned word list by downloading it to a text file on the management computer:

To download the banned word list

1. Go to **Email Filter > Content Block**.
2. Select Download.
   The FortiGate unit downloads the banned word list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

Uploading the email banned word list

You can create or edit a banned word list in a text file and upload it from your management computer to the FortiGate unit.

Each banned word or phrase must appear on a separate line in the text file. Use ASCII, Western, Chinese Simplified, Chinese Traditional, Japanese, or Korean characters. Your computer and web browser must be configured to enter characters in the character set that you use.

All words are enabled by default. Optionally, you can enter a space and a 1 after the word to enable it, and another space and a number to indicate the language.

0	Western
1	Chinese Simplified
2	Chinese Traditional
3	Japanese
4	Korean

If you do not add this information to all items in the text file, the FortiGate unit automatically enables all banned words and phrases that are followed with a 1 or no number in the Western language when you upload the text file.

Figure 42: Example Western email banned word list text file

```
banned 1 0
banned+phrase+1 1 0
“banned phrase 2” 1 0
```

To upload the banned word list

1. Go to **Email Filter > Content Block**.
2. Select Upload.
3. Type the path and filename of the banned word list text file or select Browse and locate the file.
4. Select OK to upload the banned word list text file.
   Select Return to display the banned word list.

Email block list

You can configure the FortiGate unit to tag all IMAP and POP3 protocol traffic sent from unwanted email addresses. When the FortiGate unit detects an email sent from an unwanted address pattern, the FortiGate unit adds a tag to the subject line of the email and writes a message to the email filter log. Receivers can then use their mail client software to filter messages based on the subject tag.

You can tag email from a specific sender address or from all address subdomains by adding the top-level domain name. Alternatively, you can tag email sent from individual subdomains by including the subdomain to block.

Adding address patterns to the email block list

To add an address pattern to the email block list

1. Go to **Email Filter > Block List**.
2. Select New.
3. Type a Block Pattern.
   - To tag email from a specific email address, type the email address. For example, `sender@abccompany.com`.
   - To tag email from a specific domain, type the domain name. For example, `abccompany.com`.
   - To tag email from a specific subdomain, type the subdomain name. For example, `mail.abccompany.com`.
   - To tag email from an entire organization category, type the top-level domain name. For example, type `com` to tag email sent from all organizations that use .com as the top-level domain.

   The pattern can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - (hyphen),_ (underscore), and @. Spaces and other special characters are not allowed.
4. Select OK to add the address pattern to the Email Block list.

Downloading the email block list

You can back up the email block list by downloading it to a text file on the management computer.

To download the email block list

1. Go to **Email Filter > Block List**.
2. Select Download.

   The FortiGate unit downloads the list to a text file on the management computer. You can specify a location to which to download the text file as well as a name for the text file.

Uploading an email block list

You can create a email block list in a text editor and then upload the text file to the FortiGate unit. Add one pattern to each line of the text file. You can follow the pattern with a space and then a 1 to enable or a zero (0) to disable the pattern. If you do not add this information to the text file, the FortiGate unit automatically enables all patterns that are followed with a 1 or no number when you upload the text file.

Figure 43: Example email block list text file

```
mail.badsite.com 1
suredeal.org 1
user1@badsite.com 1
```

You can either create the email block list yourself, or add a block list created by a third-party email blacklist service. For example, you can subscribe to the Realtime Blackhole List service available at http://mail-abuse.org/rbl/ as a starting point for creating your own email block list. You can upload blacklists to the FortiGate unit as text files, with only minimal editing to remove comments at the top of each list and to combine the lists that you want into a single file.

Note: All changes made to the email block list using the web-based manager are lost when you upload a new list. However, you can download your current email block list, add more patterns to it using a text editor, and then upload the edited list to the FortiGate unit.

To upload the email block list

1. In a text editor, create the list of patterns to block.
2. Using the web-based manager, go to **Email Filter > Block List**.
3. Select Upload.
4. Type the path and filename of your email block list text file, or select Browse and locate the file.
5. Select OK to upload the file to the FortiGate unit.
6. Select Return to display the updated email block list.
7. You can continue to maintain the email block list by making changes to the text file and uploading it again.

Email exempt list

Add address patterns to the exempt list to allow legitimate IMAP and POP3 traffic that might otherwise be tagged by email or content blocking. For example, if the email banned word list is set to block email that contains pornography-related words and a reputable company sends email that contains these words, the FortiGate unit would normally add a subject tag to the email. Adding the domain name of the reputable company to the exempt list allows IMAP and POP3 traffic from the company to bypass email and content blocking.

Adding address patterns to the email exempt list

To add an address pattern to the email exempt list

1 Go to **Email Filter > Exempt List**.

2 Select New.

3 Type the address pattern that you want to exempt.

- To exempt email sent from a specific email address, type the email address. For example, `sender@abccompany.com`.
- To exempt email sent from a specific domain, type the domain name. For example, `abccompany.com`.
- To exempt email sent from a specific subdomain, type the subdomain name. For example, `mail.abccompany.com`.
- To exempt email sent from an entire organization category, type the top-level domain name. For example, type `net` to exempt email sent from all organizations that use .net as the top-level domain.

The pattern can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - (hyphen),_ (underscore), and @. Spaces and other special characters are not allowed.

4 Select OK to add the address pattern to the email exempt list.

Adding a subject tag

When the FortiGate unit receives email from an unwanted address or email that contains an item in the email banned word list, the FortiGate unit adds a tag to the subject line and sends the message to the destination email address. Email users can use their mail client software to filter the messages based on the subject tag.

To add a subject tag

1 Go to **Email Filter > Config**.

2 Type the Subject Tag that you want to display in the subject line of email received from unwanted addresses or that contains banned words. For example, type `Unwanted Mail`.

Note: Do not use quotation marks in the subject tags.

3 Select Apply.

The FortiGate unit adds the tag to the subject line of all unwanted email.

Logging and reporting

You can configure the FortiGate unit to log network activity from routine configuration changes and traffic sessions to emergency events. You can also configure the FortiGate unit to send alert email messages to inform system administrators about events such as network attacks, virus incidents, and firewall and VPN events.

This chapter describes:

Recording logs

You can configure logging to record logs to one or more of:

- a computer running a syslog server,
- a computer running a WebTrends firewall reporting server,
- the console.

For information about filtering the log types and activities that the FortiGate unit records, see "Filtering log messages" on page 253. For information about traffic logs, see "Configuring traffic logging" on page 254.

This section describes:

Recording logs on a remote computer

You can configure the FortiGate unit to record log messages on a remote computer. The remote computer must be configured with a syslog server.

To record logs on a remote computer

1. Go to **Log&Report > Log Setting**.
2. Select the Log to Remote Host check box to send the logs to a syslog server.
3. Type the IP address of the remote computer running syslog server software.

4 Type the port number of the syslog server.

5 Select the severity level for which you want to record log messages.

The FortiGate unit logs all levels of severity down to, but not lower than, the level you choose. For example, if you want to record emergency, alert, critical, and error messages, select Error.

See "Log message levels" on page 253.

6 Select Config Policy.

- Select the Log type for which you want the FortiGate unit to record logs.
- For each Log type, select the activities for which you want the FortiGate unit to record log messages.

For information about log types and activities, see "Filtering log messages" on page 253 and "Configuring traffic logging" on page 254.

7 Select OK.

8 Select Apply.

Recording logs on a NetIQ WebTrends server

Use the following procedure to configure the FortiGate unit to record logs on a remote NetIQ WebTrends firewall reporting server for storage and analysis. FortiGate log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with WebTrends NetIQ Security Reporting Center 2.0 and Firewall Suite 4.1. For more information, see the Security Reporting Center and Firewall Suite documentation.

Note: FortiGate traffic log messages include sent and received fields, which are optional but required for drawing a WebTrends graph.

To record logs on a NetIQ WebTrends server

1 Go to **Log&Report > Log Setting**.

2 Select the Log in WebTrends Enhanced Log Format check box.

3 Type the IP address of the NetIQ WebTrends firewall reporting server.

4 Select the severity level for which you want to record log messages.

The FortiGate logs all levels of severity down to, but not lower than, the level you choose. For example, if you want to record emergency, alert, critical, and error messages, select Error.

See "Log message levels" on page 253.

5 Select Config Policy.

To configure the FortiGate unit to filter the types of logs and events to record, use the procedures in "Filtering log messages" on page 253 and "Configuring traffic logging" on page 254.

6 Select OK.

7 Select Apply.

Log message levels

Table 23 lists and describes FortiGate log message levels.

Table 23: FortiGate log message levels

Levels	Description	Generated by
0 - Emergency	The system has become unstable.	Emergency messages not available.
1 - Alert	Immediate action is required.	NIDS attack log messages.
2 - Critical	Functionality is affected.	DHCP
3 - Error	An error condition exists and functionality could be affected.	Error messages not available.
4 - Warning	Functionality could be affected.	Antivirus, Web filter, email filter, and system event log messages.
5 - Notice	Information about normal events.	Antivirus, Web filter, and email filter log messages.
6 - Information	General information about system operations.	Antivirus, Web filter, email filter log messages, and other event log messages.

Filtering log messages

You can configure the logs that you want to record and the message categories that you want to record in each log.

To filter log entries

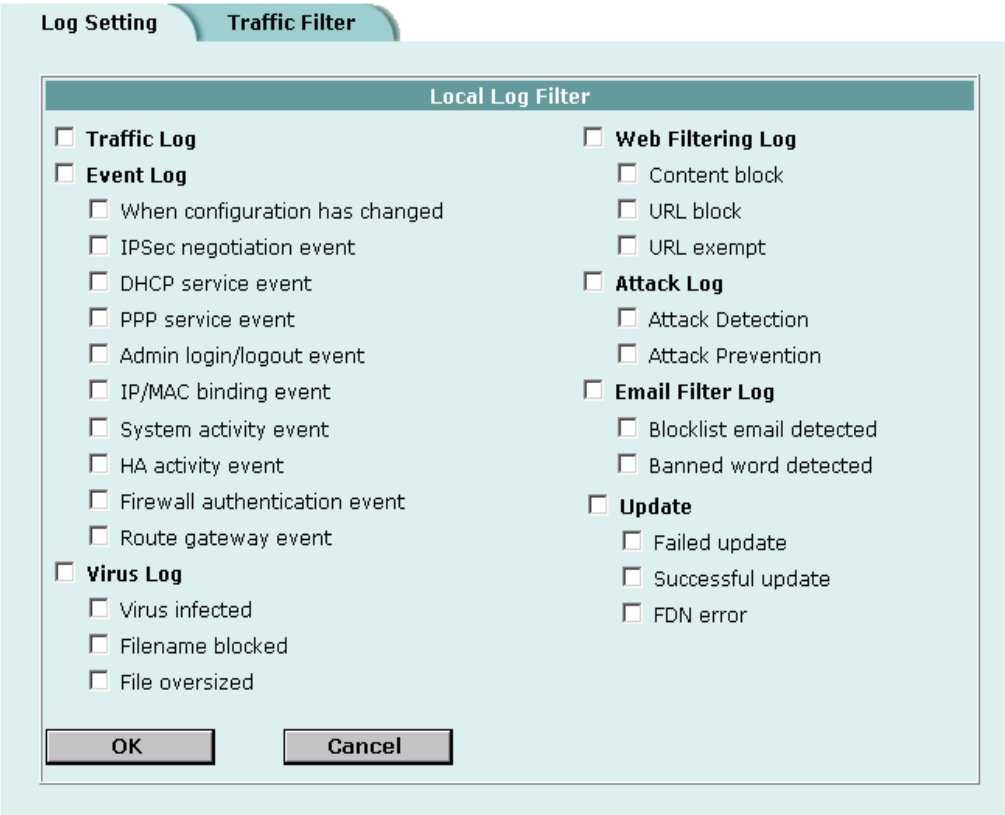
1. Go to **Log&Report > Log Setting**.
2. Select Config Policy for the log location that you selected in "Recording logs" on page 251.
3. Select the log types that you want the FortiGate unit to record.

Traffic Log	Record all connections to and through the interface. To configure traffic filtering, see "Adding traffic filter entries" on page 256.
Event Log	Record management and activity events in the event log. Management events include changes to the system configuration as well as administrator and user logins and logouts. Activity events include system activities, such as VPN tunnel establishment and HA failover events.
Virus Log	Record virus intrusion events, such as when the FortiGate unit detects a virus, blocks a file type, or blocks an oversized file or email.
Web Filtering Log	Record activity events, such as URL and content blocking, and exemption of URLs from blocking.
Attack Log	Record attacks detected by the NIDS and prevented by the NIDS Prevention module.
Email Filter Log	Record activity events, such as detection of email that contains unwanted content and email from unwanted senders.
Update	Record log messages when the FortiGate connects to the FDN to download antivirus and attack updates.

4 Select the message categories that you want the FortiGate unit to record if you selected Event Log, Virus Log, Web Filtering Log, Attack Log, Email Filter Log, or Update in step 3.

5 Select OK.

Figure 44: Example log filter configuration



Configuring traffic logging

You can configure the FortiGate unit to record traffic log messages for connections to:

- An interface
- A firewall policy

The FortiGate unit can filter traffic logs for a source and destination address and service. You can also enable the following global settings:

- resolve IP addresses to host names,
- display the port number or service.

The traffic filter list displays the name, source address and destination address, and the protocol type of the traffic to be filtered.

This section describes:

Enabling traffic logging

You can enable logging on any interface and firewall policy.

Enabling traffic logging for an interface

If you enable traffic logging for an interface, all connections to and through the interface are recorded in the traffic log.

To enable traffic logging for an interface

1. Go to **System > Network > Interface**.
2. Select Edit  in the Modify column beside the interface for which you want to enable logging.
3. For Log, select Enable.
4. Select OK.
5. Repeat this procedure for each interface for which you want to enable logging.

Enabling traffic logging for a firewall policy

If you enable traffic logging for a firewall policy, all connections accepted by the firewall policy are recorded in the traffic log.

To enable traffic logging for a firewall policy

1. Go to **Firewall > Policy**.
2. Select a policy tab.
3. Select Log Traffic.
4. Select OK.

Configuring traffic filter settings

You can configure the information recorded in all traffic log messages.

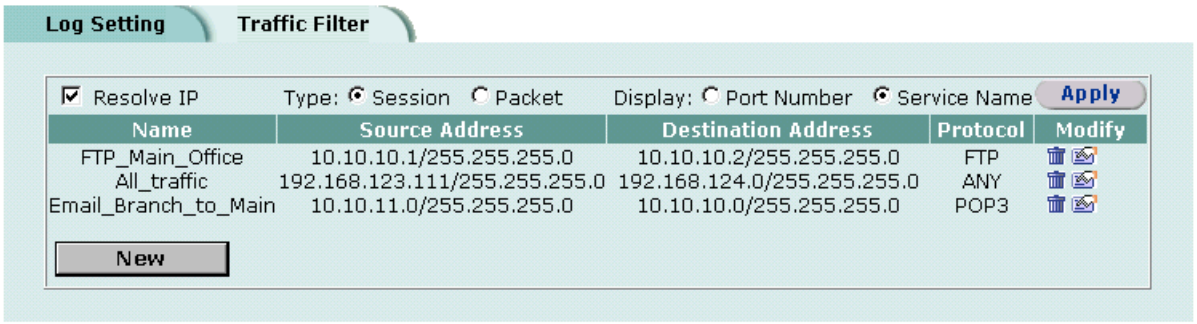
To configure traffic filter settings

1. Go to **Log&Report > Log Setting > Traffic Filter**.
2. Select the settings that you want to apply to all traffic log messages.

Resolve IP	Select Resolve IP if you want traffic log messages to list the IP address and domain name stored on the DNS server. If the primary and secondary DNS server addresses provided to you by your ISP have not already been added, go to **System > Network > DNS** and add the addresses.
Display	Select Port Number if you want traffic log messages to list the port number, for example, 80/tcp. Select Service Name if you want traffic log messages to list the name of the service, for example, TCP.

3 Select Apply.

Figure 45: Example traffic filter list



Adding traffic filter entries

Add entries to the traffic filter list to filter the messages that are recorded in the traffic log. If you do not add any entries to the traffic filter list, the FortiGate unit records all traffic log messages. You can add entries to the traffic filter list to limit the traffic logs that are recorded. You can log traffic with a specified source IP address and netmask, to a destination IP address and netmask, and for a specified service. A traffic filter entry can include any combination of source and destination addresses and services.

To add an entry to the traffic filter list

1 Go to **Log&Report > Log Setting > Traffic Filter**.

2 Select New.

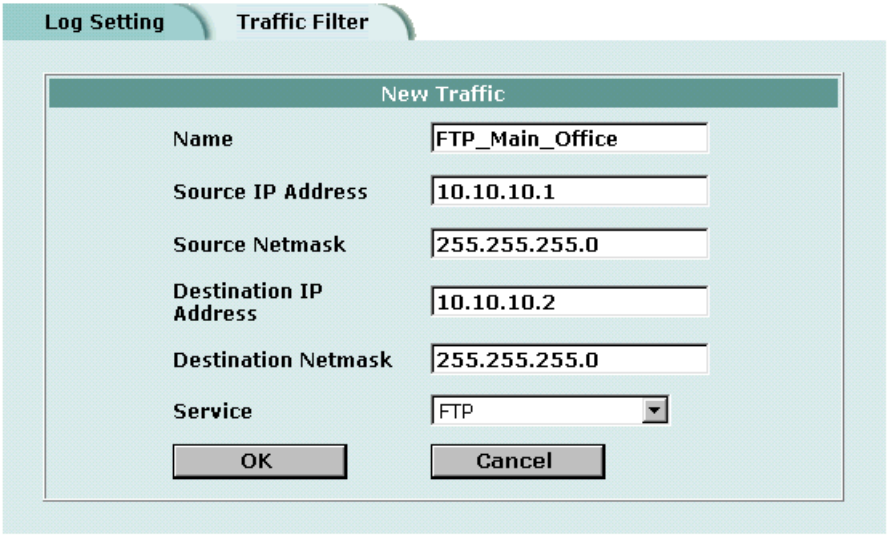
3 Configure the traffic filter for the type of traffic that you want to record on the traffic log.

Name	Type a name to identify the traffic filter entry. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Spaces and other special characters are not allowed.
Source IP Address **Source Netmask**	Type the source IP address and netmask for which you want the FortiGate unit to log traffic messages. The address can be an individual computer, subnetwork, or network.
Destination IP Address **Destination Netmask**	Type the destination IP address and netmask for which you want the FortiGate unit to log traffic messages. The address can be an individual computer, subnetwork, or network.
Service	Select the service group or individual service for which you want the FortiGate unit to log traffic messages.

4 Select OK.

The traffic filter list displays the new traffic address entry with the settings that you selected in “Enabling traffic logging” on page 255.

Figure 46: Example new traffic address entry



Configuring alert email

You can configure the FortiGate unit to send alert email to up to three email addresses when there are virus incidents, block incidents, network intrusions, and other firewall or VPN events or violations. After you set up the email addresses, you can test the settings by sending test email.

- Adding alert email addresses
- Testing alert email
- Enabling alert email

Adding alert email addresses

Because the FortiGate unit uses the SMTP server name to connect to the mail server, the FortiGate unit must look up this name on your DNS server. Before you configure alert email, make sure that you configure at least one DNS server.

To add a DNS server

1. Go to **System > Network > DNS**.
2. If they are not already there, type the primary and secondary DNS server addresses provided by your ISP.
3. Select Apply.

To add alert email addresses

1. Go to **Log&Report > Alert Mail > Configuration**.
2. Select the Authentication check box if your email server requires an SMTP password.

3 In the SMTP Server field, type the name of the SMTP server where you want the FortiGate unit to send email, in the format `smtp.domain.com`.
The SMTP server can be located on any network connected to the FortiGate unit.

4 In the SMTP User field, type a valid email address in the format `user@domain.com`.
This address appears in the From header of the alert email.

5 In the Password field, type the password that the SMTP user needs to access the SMTP server.
A password is required if you select Authentication.

6 Type up to three destination email addresses in the Email To fields.
These are the email addresses to which the FortiGate unit sends alert email.

7 Select Apply.

Testing alert email

You can test the alert email settings by sending a test email.

To send a test email

1 Go to **Log&Report > Alert Mail > Configuration**.

2 Select Test to send test email messages from the FortiGate unit to the Email To addresses.

Enabling alert email

You can configure the FortiGate unit to send alert email in response to virus incidents, intrusion attempts, and critical firewall or VPN events or violations. If you have configured logging to a local disk, you can enable sending an alert email when the hard disk is almost full.

To enable alert email

1 Go to **Log&Report > Alert Mail > Categories**.

2 Select Enable alert email for virus incidents.
Alert email is not sent when antivirus file blocking deletes a file.

3 Select Enable alert email for block incidents to have the FortiGate unit send an alert email when it blocks files affected by viruses.

4 Select Enable alert email for intrusions to have the FortiGate unit send an alert email to notify the system administrator of attacks detected by the NIDS.

5 Select Enable alert email for critical firewall/VPN events or violations to have the FortiGate unit send an alert email when a critical firewall or VPN event occurs.
Critical firewall events include failed authentication attempts.
Critical VPN events include when replay detection detects a replay packet. Replay detection can be configured for both manual key and AutoIKE Key VPN tunnels.

6 Select Send alert email when disk is full to have the FortiGate unit send an alert email when the hard disk is almost full.

7 Select Apply.

Glossary

Connection: A link between machines, applications, processes, and so on that can be logical, physical, or both.

DMZ, Demilitarized Zone: 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 (HTTP) servers, FTP servers, SMTP (email) servers and DNS servers.

DMZ interface: The FortiGate interface that is connected to a DMZ network.

DNS, Domain Name Service: A service that converts symbolic node names to IP addresses.

Ethernet: A local-area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps. Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100 Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet, supports data rates of 1 gigabit (1,000 megabits) per second.

External interface: The FortiGate interface that is connected to the Internet. For the FortiGate-60 the external interface is WAN1 or WAN2.

FTP, File transfer Protocol: An application and TCP/IP protocol used to upload or download files.

Gateway: A combination of hardware and software that links different networks. Gateways between TCP/IP networks, for example, can link different subnetworks.

HTTP, Hyper Text Transfer 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 SSL protocol for transmitting private documents over the Internet using a Web browser.

Internal interface: The FortiGate interface that is connected to an internal (private) network.

Internet: A collection of networks connected together that span the entire globe using the NFSNET as their backbone. As a generic term, it refers to any collection of interdependent networks.

ICMP, Internet Control Message Protocol: Part of the Internet Protocol (IP) that allows for the generation of error messages, test packets, and information messages relating to IP. This is the protocol used by the ping function when sending ICMP Echo Requests to a network host.

IKE, Internet Key Exchange: A method of automatically exchanging authentication and encryption keys between two secure servers.

IMAP, Internet Message Access Protocol: An Internet email protocol that allows access to your email from any IMAP compatible browser. With IMAP, your mail resides on the server.

IP, Internet Protocol: The component of TCP/IP that handles routing.

IP Address: An identifier for a computer or device on a TCP/IP network. An IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

L2TP, Layer Two (2) Tunneling Protocol: An extension to the PPTP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges PPTP from Microsoft and L2F from Cisco Systems. To create an L2TP VPN, your ISP's routers must support L2TP.

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.

LAN, Local Area Network: A computer network that spans a relatively small area. Most LANs connect workstations and personal computers. Each computer on a LAN is able to access data and devices anywhere on the LAN. This means that many users can share data as well as physical resources such as printers.

MAC address, Media Access Control address: A hardware address that uniquely identifies each node of a network.

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 being sent. Ideally, you want the MTU your network produces to be the same as the smallest MTU of all the networks between your machine and a message's final destination. If your messages are larger than one of the intervening MTUs, they get broken up (fragmented), which slows down transmission speeds.

Netmask: Also called subnet mask. A set of rules for omitting parts of a complete IP address to reach a target destination without using a broadcast message. It can indicate a subnetwork portion of a larger network in TCP/IP. Sometimes referred to as an Address Mask.

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 (UTC).

Packet: A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Ping, Packet Internet Grouper: A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

POP3, Post Office Protocol: A protocol used to transfer e-mail from a mail server to a mail client across the Internet. Most e-mail clients use POP.

PPP, Point-to-Point Protocol: A TCP/IP protocol that provides host-to-network and router-to-router connections.

PPTP, Point-to-Point Tunneling Protocol: A Windows-based technology for creating VPNs. PPTP is supported by Windows 98, 2000, and XP. To create a PPTP VPN, your ISP's routers must support PPTP.

Port: In TCP/IP and UDP networks, a port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Protocol: An agreed-upon format for transmitting data between two devices. 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**: An authentication and accounting system used by many Internet Service Providers (ISPs). When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Router: A device that connects LANs into an internal network and routes traffic between them.

Routing: The process of determining a path to use to send data to its destination.

Routing table: A list of valid paths through which data can be transmitted.

Server: An application that answers requests from other devices (clients). Used as a generic term for any device that provides services to the rest of the network such as printing, high capacity storage, and network access.

SMTP, Simple Mail Transfer Protocol: In TCP/IP networks, this is an application for providing mail delivery services.

SNMP, **Simple Network Management Protocol**: A set of protocols for managing networks. SNMP works by sending messages to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SSH, **Secure shell**: A secure Telnet replacement that you can use to log into another computer over a network and run commands. SSH provides strong secure authentication and secure communications over insecure channels.

Subnet: A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

Subnet Address: The part of the IP address that identifies the subnetwork.

TCP, Transmission Control Protocol: One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

UDP, User Datagram Protocol: A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.

VPN, Virtual Private Network: A network that links private networks over the Internet. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

Virus: A computer program that attaches itself to other programs, spreading itself through computers or networks by this mechanism usually with harmful intent.

Worm: A program or algorithm that replicates itself over a computer network, usually through email, and performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W