FortiGate 800/800F Installation Guide

FortiGate-800

FortiGate-800F

Version 2.80 MR6

26 October 2004

01-28006-0024-20041026

FortiGate-800/800F Installation Guide
Version 2.80 MR6
26 October 2004
01-28006-0024-20041026

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

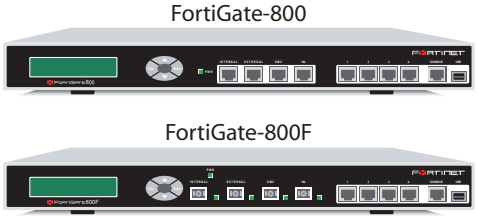
Introduction

FortiGate Antivirus Firewalls improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network. FortiGate Antivirus Firewalls are ICSA-certified for firewall, IPSec, and antivirus services.

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

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

The FortiGate Antivirus Firewall uses Fortinet's Accelerated Behavior and Content Analysis System (ABACAS™) technology, which leverages breakthroughs in chip design, networking, security, and content analysis. The unique ASIC-based architecture analyzes content and behavior in real-time, enabling key applications to be deployed right at the network edge where they are most effective at protecting your networks.



The FortiGate-800/800F model provides the performance demanded by large enterprises. Features include high throughput, a total of 8 network connections (4 user-defined), 802.1Q VLAN support, virtual domains, stateful failover HA, and support for the RIP and OSPF routing protocols. The flexibility, reliability, and easy management of the FortiGate-800/800F makes it a natural choice for enterprise applications.

Secure installation, configuration, and management

The FortiGate unit default configuration includes default interface IP addresses and is only a few steps away from protecting your network. There are several ways to configure basic FortiGate settings:

- the web-based manager,
- the front panel front keypad and LCD,
- the command line interface (CLI), or
- the setup wizard.

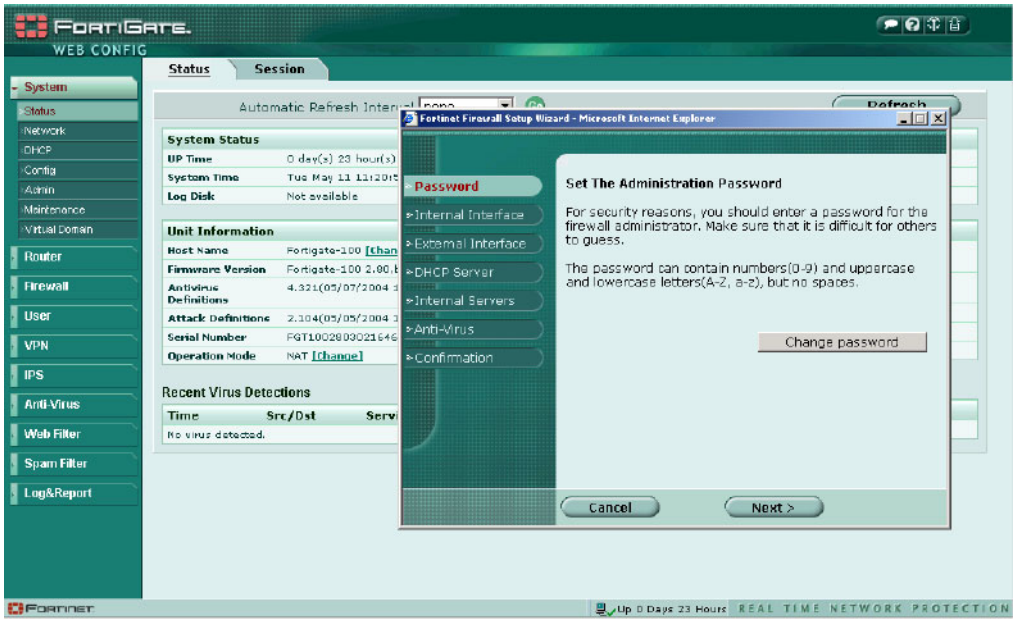
The CLI or the web-based manager can then be used to complete configuration and to perform maintenance and administration.

Web-based manager

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

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

Figure 1: FortiGate web-based manager and setup wizard



Command line interface

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

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

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

Setup wizard

The FortiGate setup wizard provides an easy way to configure the basic initial settings for the FortiGate unit. The wizard walks through the configuration of a new administrator password, FortiGate interfaces, DHCP server settings, internal servers (web, FTP, etc.), and basic antivirus settings.

Document conventions

This guide uses the following conventions to describe command syntax.

- Angle brackets `< >` to indicate variables.

  For example:

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

  You enter:

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

  `<xxx_str>` indicates an ASCII string that does not contain new-lines or carriage returns.

  `<xxx_integer>` indicates an integer string that is a decimal (base 10) number.

  `<xxx_octet>` indicates a hexadecimal string that uses the digits 0-9 and letters A-F.

  `<xxx_ipv4>` indicates a dotted decimal IPv4 address.

  `<xxx_v4mask>` indicates a dotted decimal IPv4 netmask.

  `<xxx_ipv4mask>` indicates a dotted decimal IPv4 address followed by a dotted decimal IPv4 netmask.

  `<xxx_ipv6>` indicates a dotted decimal IPv6 address.

  `<xxx_v6mask>` indicates a dotted decimal IPv6 netmask.

  `<xxx_ipv6mask>` indicates a dotted decimal IPv6 address followed by a dotted decimal IPv6 netmask.
- Vertical bar and curly brackets `{|}` to separate alternative, mutually exclusive required keywords.

  For example:

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

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

  For example:

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

  To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the internal interface, you can enter `show system interface internal`.
- A space to separate options that can be entered in any combination and must be separated by spaces.

  For example:

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

You can enter any of the following:

```
set allowaccess ping
set allowaccess ping https ssh
set allowaccess https ping ssh
set allowaccess snmp
```

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

FortiGate documentation

Information about FortiGate products is available from the following guides:

- *FortiGate QuickStart Guide*

  Provides basic information about connecting and installing a FortiGate unit.

- *FortiGate Installation Guide*

  Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.

- *FortiGate Administration Guide*

  Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.

- *FortiGate online help*

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

- *FortiGate CLI Reference Guide*

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

- *FortiGate Log Message Reference Guide*

  Describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.

- *FortiGate High Availability Guide*

  Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.

Related documentation

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

FortiManager documentation

- *FortiManager QuickStart Guide*

  Explains how to install the FortiManager Console, set up the FortiManager Server, and configure basic settings.
- *FortiManager System Administration Guide*

  Describes how to use the FortiManager System to manage FortiGate devices.
- *FortiManager System online help*

  Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the FortiManager Console as you work.

FortiClient documentation

- *FortiClient Host Security User Guide*

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

  Provides information and procedures for using and configuring the FortiClient software.

FortiMail documentation

- *FortiMail Administration Guide*

  Describes how to install, configure, and manage a FortiMail unit in gateway mode and server mode, including how to configure the unit; create profiles and policies; configure antispam and antivirus filters; create user accounts; and set up logging and reporting.
- *FortiMail online help*

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

  Describes how to use the FortiMail web-based email client, including how to send and receive email; how to add, import, and export addresses; and how to configure message display preferences.

FortiLog documentation

- *FortiLog Administration Guide*

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

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

The FortiGate online help also contains procedures for using the FortiGate web-based manager to configure and manage the FortiGate unit. For a complete list of FortiGate documentation visit Fortinet Technical Support at http://support.fortinet.com.

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 change 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 section describes unpacking, setting up, and powering on a FortiGate Antivirus Firewall unit. This section includes:

Package contents

The FortiGate-800 and FortiGate-800F package contains the following items:

- FortiGate-800 or FortiGate-800F Antivirus Firewall
- one orange crossover ethernet cable (Fortinet part number CC300248)
- one grey regular ethernet cable (Fortinet part number CC300249)
- one RJ-45 to DB-9 serial cable
- SFP transceivers (FortiGate-800F only)
- one power cable
- two 19-inch rack mount brackets
- FortiGate-800 or FortiGate-800F QuickStart Guide
- CD containing Fortinet user documentation

Figure 2: FortiGate-800 package contents

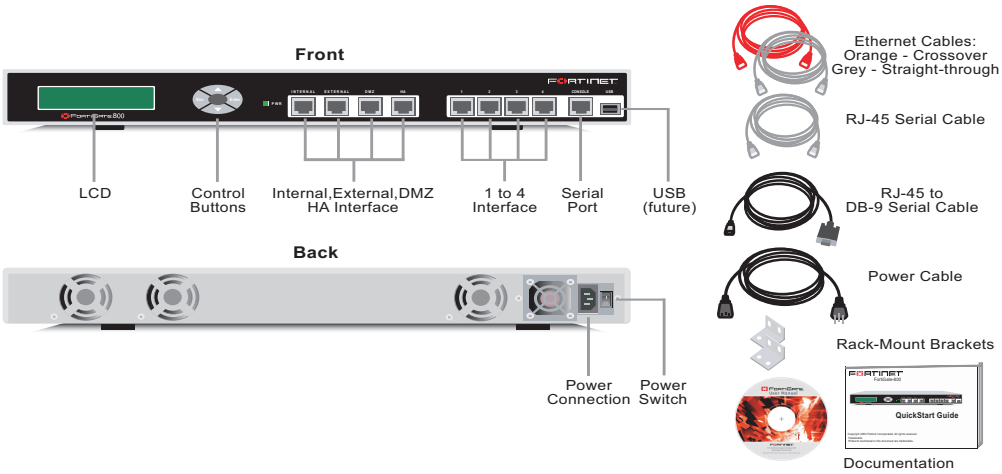
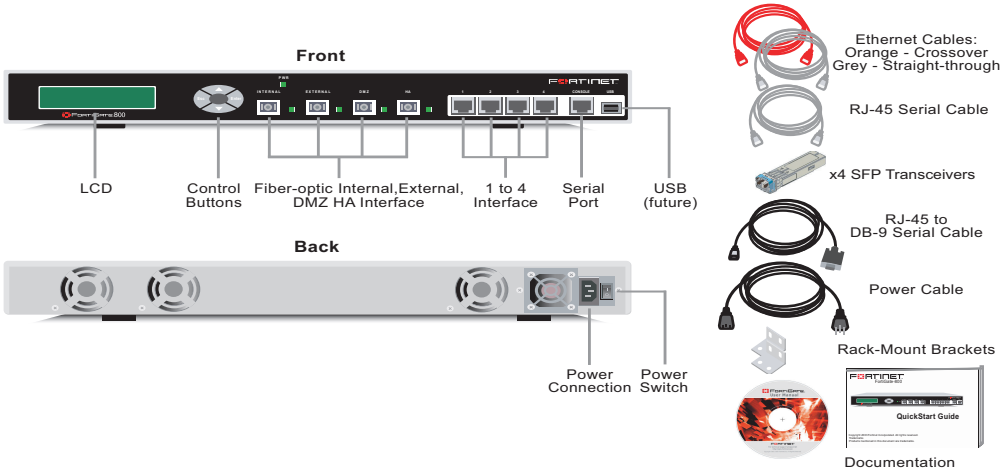


Figure 3: FortiGate-800F package contents



Mounting

The FortiGate-800/800F unit can be mounted in a standard 19-inch rack. It requires 1 U of vertical space in the rack.

The FortiGate-800/800F unit can also be installed as a free-standing appliance on any stable surface.

Dimensions

- 16.75 x 12 x 1.75 in. (42.7 x 30.5 x 4.5 cm)

Weight

- 10 lb. (4.5 kg)

Power requirements

- Power dissipation: 300 W (max)
- AC input voltage: 100 to 240 VAC
- AC input current: 6 A
- Frequency: 50 to 60 Hz
- The FortiGate-800/800F unit may overload your supply circuit and impact your overcurrent protection and supply wiring. Use appropriate equipment nameplate ratings to address this concern.
- Make sure that the FortiGate-800/800F unit has reliable grounding. Fortinet recommends direct connections to the branch circuit.

Environmental specifications

- Operating temperature: 41 to 95°F (5 to 35°C)
- Storage temperature: -4 to 176°F (-20 to 80°C)
- Humidity: 10 to 90% non-condensing
- If you install the FortiGate-800/800F unit in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Make sure the operating ambient temperature does not exceed the manufacturer's maximum rated ambient temperature.

Air flow

- For rack installation, make sure that the amount of air flow required for safe operation of the FortiGate unit is not compromised.
- For free-standing installation, make sure that the FortiGate unit has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Mechanical loading

- For rack installation, make sure the mechanical loading of the FortiGate unit is evenly distributed to avoid a hazardous condition.

Turning the FortiGate unit power on and off

Table 1: FortiGate-800 LED indicators

LED	State	Description
Power	Green	The FortiGate unit is powered on.
	Off	The FortiGate unit is powered off.
Internal **External** **DMZ** **HA** **1 to 4**	Amber	The correct cable is in use and the connected equipment has power.
	Flashing amber	Network activity at this interface.
	Green	The interface is connected. Internal, External, DMZ and HA connect at up to 1000 Mbps. Interfaces 1, 2, 3 and 4 connect at up to 100 Mbps.
	Off	No link established.

Table 2: FortiGate-800F LED indicators

LED	State	Description
Power	Green	The FortiGate-800F unit is powered on.
	Off	The FortiGate-800F unit is powered off.
Internal **External** **DMZ** **HA**	Amber	The correct cable is in use and the connected equipment has power.
	Flashing Amber	Network activity at this interface.
	Off	No link established.

To power off the FortiGate unit

Always shut down the FortiGate operating system properly before turning off the power switch.

1. From the web-based manager, go to **System > Maintenance > ShutDown**, select Shut Down and select Apply, or from the CLI, enter:

```
execute shutdown
```

2. Turn off the power switch.
3. Disconnect the power cable from the power supply.

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 6.0 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 6.0 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 with a netmask of 255.255.255.0.
2. Start Internet Explorer and browse to the address https://192.168.1.99. (remember to include the “s” in https://).
   The FortiGate login is displayed.

Figure 4: FortiGate login

3. Type admin in the Name field and select 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 RJ-45 serial cable included in your FortiGate package,
- the RJ-45 to DB-9 convertor included in your FortiGate package (if required),
- 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 serial cable to the communications port of your computer and to the FortiGate Console port.
   Use the RJ-45 to DB-9 convertor if your PC communications port requires a DB-9 connector.
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 your computer 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-800 login:
   ```
   or
   ```
   FortiGate-800F login:
   ```
7. Type `admin` and press Enter twice.
   The following prompt is displayed:
   ```
   Welcome !
   ```
   Type ? to list available 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 basic 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 protection profiles can be used to apply different levels of antivirus protection, web content filtering, spam filtering, and IPS to the network traffic that is controlled by firewall policies.

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 administrative access means you can connect to the web-based manager using HTTPS protocol through this interface. Ping administrative 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: Administrative Access:	192.168.1.99 255.255.255.0 HTTPS, Ping
External interface	IP: Netmask: Administrative Access:	192.168.100.99 255.255.255.0 Ping
DMZ interface	IP: Netmask: Administrative Access:	10.10.10.1 255.255.255.0 HTTPS, Ping

Table 3: Factory default NAT/Route mode network configuration (Continued)

HA interface	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping
Port 1	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping
Port 2	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping
Port 3	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping
Port 4	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping
Network Settings	Default Gateway (for default route)	192.168.100.1
	Interface connected to external network (for default route)	external
	Default Route A default route consists of a default gateway and the name of the interface connected to the external network (usually the Internet). The default gateway directs all non-local traffic to this interface and to the external network.	
	Primary DNS Server	207.192.200.1
	Secondary DNS Server	207.192.200.129

Factory default Transparent mode network configuration

In Transparent mode, the FortiGate unit 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

Table 4: Factory default Transparent mode network configuration (Continued)

Administrative access	Internal	HTTPS, Ping
	External	Ping
	DMZ	HTTPS, Ping
	Port 1	Ping
	Port 2	Ping
	Port 3	Ping
	Port 4	Ping

Factory default firewall configuration

FortiGate firewall policies control how all traffic is processed by the FortiGate unit. Until firewall policies are added, no traffic can be accepted by or pass through the FortiGate unit. To allow traffic through the FortiGate unit you can add firewall policies. See the *FortiGate Administration Guide* for information about adding firewall policies.

The following firewall configuration settings are included in the default firewall configuration to make it easier to add firewall policies.

Table 5: Default firewall configuration

Configuration setting	Name	Description
Firewall address	All	Firewall address matches the source or destination address of any packet.
Pre-defined service	More than 50 predefined services	Select from any of the 50 pre-defined services to control traffic through the FortiGate unit that uses that service.
Recurring schedule	Always	The recurring schedule is valid at any time.
Protection Profiles	Strict, Scan, Web, Unfiltered	Control how the FortiGate unit applies virus scanning, web content filtering, spam filtering, and IPS.

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

Factory default protection profiles

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

- Configure antivirus protection for HTTP, FTP, IMAP, POP3, and SMTP firewall policies
- Configure Web filtering for HTTP firewall policies
- Configure Web category filtering for HTTP firewall policies
- Configure spam filtering for IMAP, POP3, and SMTP firewall policies
- Enable the Intrusion Protection System (IPS) for all services
- Enable content logging for HTTP, FTP, IMAP, POP3, and SMTP firewall policies

Using protection 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 firewall policies for different traffic services to use the same or different protection profiles.

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

The FortiGate unit comes preconfigured with four protection profiles.

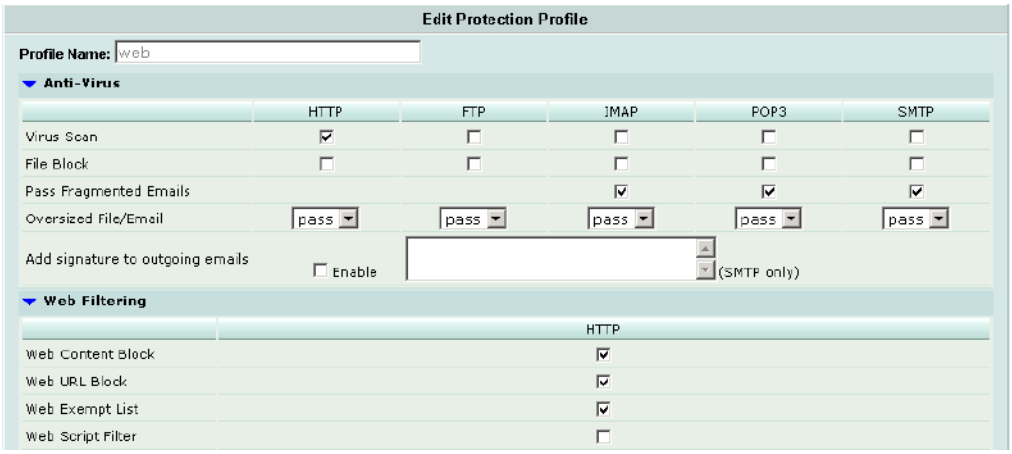
Strict To apply maximum protection to HTTP, FTP, IMAP, POP3, and SMTP traffic. You may not use the strict protection profile under normal circumstances but it is available if you have problems with viruses and require maximum screening.

Scan To apply antivirus scanning to HTTP, FTP, IMAP, POP3, and SMTP content traffic. Quarantine is also selected for all content services. On FortiGate models with a hard drive, if antivirus scanning finds a virus in a file, the file is quarantined on the FortiGate local disk. If required, system administrators can recover quarantined files.

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

Unfiltered To apply no scanning, blocking or IPS. Use if you do not want to apply content protection to content traffic. You can add this protection profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected.

Figure 5: Web protection profile settings



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 FortiGate 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:

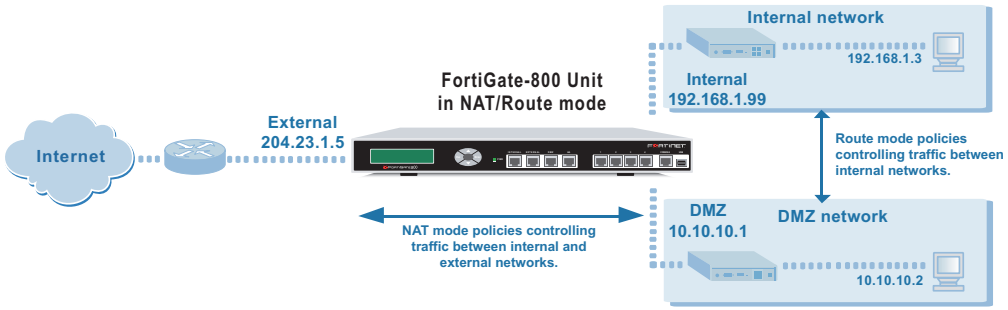
- External is the interface to the external network (usually the Internet).
- Internal is the interface to the internal network.
- DMZ is the interface to the DMZ network.
- HA is the interface used to connect to other FortiGate-800/800F units if you are installing an HA cluster
- Ports 1 to 4 can be connected to other networks.

You can add firewall policies to control whether communications through the FortiGate unit operate in NAT or Route mode. Firewall 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 address translation.

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 firewall policies to control traffic flowing between the internal, private network and the external, public network (usually the Internet).

If you have multiple internal networks, such as a DMZ network in addition to the internal, private network, you could create route mode firewall policies for traffic flowing between them.

Figure 6: Example NAT/Route mode network configuration



NAT/Route mode with multiple external network connections

In NAT/Route mode, you can configure the FortiGate unit with multiple redundant connections to the external network (usually the Internet). For example, you could create the following configuration:

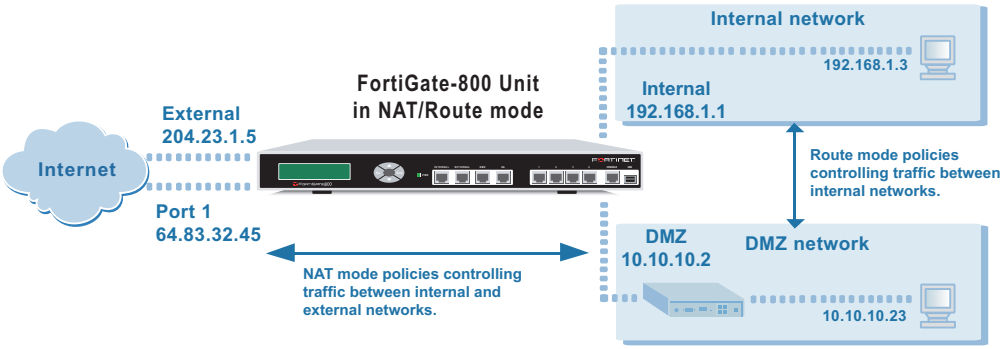
- External is the default interface to the external network (usually the Internet).
- Port 1 is the redundant interface to the external network.
- Internal is the interface to the internal network.
- DMZ is the interface to the DMZ network.

You must configure routing to support redundant Internet connections. Routing can be used to automatically redirect connections from an interface if its connection to the external network fails.

Otherwise, security policy configuration is similar to a NAT/Route mode configuration with a single Internet connection. You would create NAT mode firewall policies to control traffic flowing between the internal, private network and the external, public network (usually the Internet).

If you have multiple internal networks, such as a DMZ network in addition to the internal, private network, you could create route mode firewall policies for traffic flowing between them.

Figure 7: Example NAT/Route multiple internet connection configuration

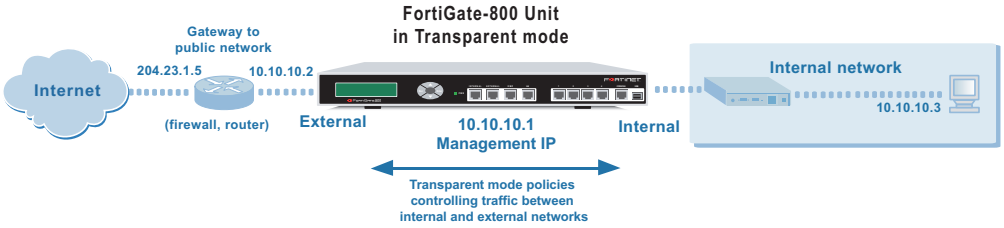


Transparent mode

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, IPSec VPN, virus scanning, IPS, web content filtering, and Spam filtering.

Figure 8: Example Transparent mode network configuration



You can connect up to 8 network segments to the FortiGate unit to control traffic between these network segments.

- External can connect to the external firewall or router.
- Internal can connect to the internal network.
- HA can connect to another network or to other FortiGate-800/800F units if you are installing an HA cluster.
- DMZ and ports 1 to 4 can connect to other network segments.

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. Choose among three different tools to configure the FortiGate unit

Web-based manager and setup wizard

The FortiGate web-based manager is a full featured management tool. You can use the web-based manager to configure most FortiGate settings.

The web-based manager Setup Wizard guides you through the initial configuration steps. Use the Setup Wizard to configure the administrator password, the interface addresses, the default gateway address, and the DNS server addresses. Optionally, use the Setup Wizard to configure the internal server settings for NAT/Route mode.

To connect to the web-based manager you require:

- Ethernet connection between the FortiGate unit and a management computer.
- Internet Explorer version 6.0 or higher on the management computer.

CLI

The FortiGate CLI is a full-featured management tool. Use it to configure the administrator password, the interface addresses, the default gateway address, and the DNS server addresses. To connect to the CLI you require:

- Serial connection between the FortiGate unit and a management computer.
- A terminal emulation application on the management computer.

Front control buttons and LCD

If you are configuring the FortiGate unit to operate in NAT/Route mode, you can use the front keypad and LCD to add the IP address of the FortiGate interfaces as well as the external default gateway.

If you are configuring the FortiGate unit to operate in Transparent mode, you can use the front keypad and LCD to switch to Transparent mode. Then you can add the management IP address and default gateway.

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.

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 27.
- If you are going to operate the FortiGate unit in Transparent mode, go to "Transparent mode installation" on page 41.
- If you are going to operate two or more FortiGate units in HA mode, go to "High availability installation" on page 51.

NAT/Route mode installation

This chapter describes how to install the FortiGate unit in NAT/Route mode. For information about installing a FortiGate unit in Transparent mode, see "Transparent mode installation" on page 41. For information about installing two or more FortiGate units in HA mode, see "High availability installation" on page 51. For more information about installing the FortiGate unit in NAT/Route mode, see "Planning the FortiGate configuration" on page 23.

This chapter describes:

Preparing to configure the FortiGate unit in NAT/Route mode

Use Table 6 to gather the information that you need to customize NAT/Route mode settings.

You can configure the FortiGate unit in several ways:

- the web-based manager GUI is a complete interface for configuring most settings. See "Using the web-based manager" on page 29.
- the front control buttons and LCD provide access to basic settings "Using the front control buttons and LCD" on page 30.
- the command line interface (CLI) is a complete text-based interface for configuring all settings. See "Using the command line interface" on page 31.
- the setup wizard provides easy, fast configuration of the most basic settings to get the unit up and running quickly. See "Using the setup wizard" on page 34.

The method that you choose depends on the complexity of the configuration, access and equipment, and the type of interface you are most comfortable using.

Table 6: NAT/Route mode settings

Administrator Password:		
Internal	IP: Netmask:	_____.____.____.____ _____.____.____.____
External	IP: Netmask:	_____.____.____.____ _____.____.____.____
DMZ	IP: Netmask:	_____.____.____.____ _____.____.____.____
HA	IP: Netmask:	_____.____.____.____ _____.____.____.____
Port 1	IP: Netmask:	_____.____.____.____ _____.____.____.____
Port 2	IP: Netmask:	_____.____.____.____ _____.____.____.____
Port 3	IP: Netmask:	_____.____.____.____ _____.____.____.____
Port 4	IP: Netmask:	_____.____.____.____ _____.____.____.____
Network settings	Default Gateway: Interface connected to external network (usually external):	_____.____.____.____
	A default route consists of a default gateway and the name of the interface connected to the external network (usually the Internet). The default gateway directs all non-local traffic to this interface and to the external network.	
	Primary DNS Server: Secondary DNS Server:	_____.____.____.____ _____.____.____.____

DHCP or PPPoE configuration

You can configure any FortiGate interface to acquire its IP address from a DHCP or PPPoE server. Your ISP may provide IP addresses using one of these protocols.

To use the FortiGate DHCP server, you need to configure an IP address range and default route for the server. No configuration information is required for interfaces that are configured to use DHCP.

PPPoE requires you to supply a user name and password. In addition, PPPoE unnumbered configurations require you to supply an IP address. Use Table 7 to record the information you require for your PPPoE configuration.

Table 7: PPPoE settings

User name:	
Password:	

Using the web-based manager

You can use the web-based manager for the initial configuration of the FortiGate unit. You can also continue to use the web-based manager for all FortiGate unit settings.

For information about connecting to the web-based manager, see "Connecting to the web-based manager" on page 16.

Configuring basic settings

After connecting to the web-based manager you can use the following procedures to complete the basic configuration of the FortiGate unit.

To add/change the administrator password

1. Go to **System > Admin > Administrators**.
2. Select the Change Password icon for the admin administrator.
3. Enter the new password and enter it again to confirm.
4. Select OK.

To configure interfaces

1. Go to **System > Network > Interface**.
2. Select the edit icon for an interface.
3. Set the addressing mode for the interface.
   Choose from manual, DHCP, or PPPoE.
4. Complete the addressing configuration.
   - For manual addressing, enter the IP address and netmask for the interface.
   - For DHCP addressing, select DHCP and any required settings.
   - For PPPoE addressing, select PPPoE, and enter the username and password and any other required settings.

   For information about how to configure these and other interface settings, see the FortiGate online help or the *FortiGate Administration Guide*.
5. Select OK.
6. Repeat this procedure for each interface.

Note: If you change the IP address of the interface you are connecting to, you must connect through a web browser again using the new address. Browse to https:// followed by the new IP address of the interface. If the new IP address of the interface is on a different subnet, you may have to change the IP address of your computer to the same subnet.

To configure DNS server settings

1 Go to **System > Network > DNS**.
2 Enter the IP address of the primary DNS server.
3 Enter the IP address of the secondary DNS server.
4 Select OK.

To add a default route

Add a default route to configure where the FortiGate unit sends traffic destined for an external network (usually the Internet). Adding the default route also defines which interface is connected to an external network. The default route is not required if the interface connected to the external network is configured using DHCP or PPPoE.

1 Go to **System > Router > Static**.
2 If the Static Route table contains a default route (IP and Mask set to 0.0.0.0), select the Delete icon to delete this route.
3 Select Create New.
4 Set Destination IP to 0.0.0.0.
5 Set Mask to 0.0.0.0.
6 Set Gateway to the default gateway IP address.
7 Set Device to the interface connected to the external network.
8 Select OK.

Using the front control buttons and LCD

Basic settings, including interface IP addresses, netmasks, default gateways, and the FortiGate operating mode can be configured using the LCD and front control buttons on the FortiGate unit. Use the information that you recorded in Table 6 on page 28 to complete the following procedure. Start when Main Menu is displayed on the LCD.

Note: You cannot configure DHCP or PPPoE from the control buttons and LCD. Instead you can use the web-based manager, the CLI, or the setup wizard.

To change the IP address and netmask of an interface

1 Press Enter to display the interface list.

2 Use the up and down arrows to highlight the name of the interface to change and press Enter.

3 Press Enter for IP address.

4 Use the up and down arrow keys to increase or decrease the value of each IP address digit. Press Enter to move to the next digit. Press Esc to move to the previous digit.

Note: When you enter an IP address, the LCD always shows three digits for each part of the address. For example, the IP address 192.168.100.1 appears on the LCD as 192.168.100.001. The IP address 192.168.23.45 appears as 192.168.023.045.

5 After you set the last digit of the IP address, press Enter.

6 Use the down arrow to highlight Netmask.

7 Press Enter and change the Netmask.

8 After you set the last digit of the Netmask, press Enter.

9 Press Esc to return to the Main Menu.

To add a default gateway to an interface

The default gateway is usually configured for the interface connected to the Internet. You can use the procedure below to configure a default gateway for any interface.

1 Press Enter to display the interface list.

2 Use the down arrow key to highlight the name of the interface connected to the Internet and press Enter.

3 Use the down arrow to highlight Default Gateway.

4 Press Enter and set the default gateway.

5 After you set the last digit of the default gateway, press Enter.

6 Press Esc to return to the Main Menu.

You have now completed the initial configuration of the FortiGate unit and you can proceed to "Next steps" on page 39.

Using the command line interface

You can also configure the FortiGate unit using the command line interface (CLI). For information about connecting to the CLI, see "Connecting to the command line interface (CLI)" on page 17.

Configuring the FortiGate unit to operate in NAT/Route mode

Use the information that you gathered in Table 6 on page 28 to complete the following procedures.

To add/change the administrator password

1 Log in to the CLI.

2 Change the admin administrator password. Enter:

```
config system admin
    edit admin
        set password <psswrd>
  end
```

To configure interfaces

1 Log in to the CLI.

2 Set the IP address and netmask of the internal interface to the internal IP address and netmask that you recorded in Table 6 on page 28. Enter:

```
config system interface
    edit internal
        set mode static
        set ip <address_ip> <netmask>
  end
```

Example

```
config system interface
    edit internal
        set mode static
        set ip <192.168.120.99> <255.255.255.0>
  end
```

3 Set the IP address and netmask of the external interface to the external IP address and netmask that you recorded in Table 6 on page 28.

```
config system external
    edit external
        set mode static
        set ip <address_ip> <netmask>
  end
```

Example

```
config system external
    edit external
        set mode static
        set ip <204.23.1.5> <255.255.255.0>
  end
```

To set the external interface to use DHCP, enter:

```
config system interface
    edit external
        set mode dhcp
  end
```

To set the external interface to use PPPoE, enter:

```
config system interface
    edit external
        set mode pppoe
        set connection enable
        set username <name_str>
        set password <psswrd>
  end
```

4 Use the same syntax to set the IP address of each FortiGate interface as required.

5 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.

To configure DNS server settings

- Set the primary and secondary DNS server IP addresses. Enter

```
config system dns
    set primary <address_ip>
    set secondary <address_ip>
  end
```

Example

```
config system dns
    set primary 293.44.75.21
    set secondary 293.44.75.22
  end
```

To add a default route

Add a default route to configure where the FortiGate unit sends traffic that should be sent to an external network (usually the Internet). Adding the default route also defines which interface is connected to an external network. The default route is not required if the interface connected to the external network is configured using DHCP or PPPoE.

- Set the default route to the Default Gateway IP address. Enter:

```
config router static
    edit 1
        set dst 0.0.0.0 0.0.0.0
        set gateway <gateway_IP>
        set device <interface>
  end
```

Example

If the default gateway IP is 204.23.1.2 and this gateway is connected to the external interface:

```
config router static
    edit 1
        set dst 0.0.0.0 0.0.0.0
        set gateway 204.23.1.2
        set device external
  end
```

Using the setup wizard

From the web-based manager, you can use the setup wizard to complete the initial configuration of the FortiGate unit. For information about connecting to the web-based manager, see “Connecting to the web-based manager” on page 16.

If you are configuring the FortiGate unit to operate in NAT/Route mode (the default), you can use the setup wizard to:

- add the administration password
- configure the internal interface address
- choose either a manual (static) or a dynamic (DHCP or PPPoE) address for the external interface
- add a default route for the external interface
- add the DNS server IP addresses
- add the DHCP server settings and IP addresses
- add various internal server IP addresses including web, IMAP, POP3, SMTP, and FTP servers
- set the antivirus protection to high, medium, or none

Table 8 lists the additional settings that you can configure with the setup wizard. See Table 6 on page 28 and Table 7 on page 29 for other settings.

Table 8: Setup wizard settings

Password	Prepare an administrator password.	
Internal Interface	Use the information you gathered in Table 6 on page 28.	
External Interface	Use the information you gathered in Table 6 on page 28.	
DHCP server	Starting IP:	_____ . _____ . _____ . _____
	Ending IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
	Default Gateway:	_____ . _____ . _____ . _____
	DNS IP:	_____ . _____ . _____ . _____
	Your FortiGate firewall contains a DHCP server to automatically set up the addresses of computers on your internal network	
Internal servers	Web Server:	_____ . _____ . _____ . _____
	SMTP Server:	_____ . _____ . _____ . _____
	POP3 Server:	_____ . _____ . _____ . _____
	IMAP Server:	_____ . _____ . _____ . _____
	FTP Server:	_____ . _____ . _____ . _____
	If you provide access from the Internet to a web server, SMTP server, POP3 server IMAP server, or FTP server installed on an internal network, add the IP addresses of the servers here.	
Antivirus	High	Create a protection profile that enables virus scanning, file blocking, and blocking of oversize email for HTTP, FTP, IMAP, POP3, and SMTP. Add this protection profile to a default firewall policy.
	Medium	Create a protection profile that enables virus scanning, for HTTP, FTP, IMAP, POP3, and SMTP (recommended). Add this protection profile to a default firewall policy.
	None	Do not configure antivirus protection.
	Select one of these security levels to protect your network from viruses.	

Starting the setup wizard

1 In the web-based manager, select Easy Setup Wizard.

Figure 9: Select the Easy Setup Wizard

2 Follow the instructions on the wizard pages and use the information that you gathered in Table 6 on page 28 and Table 8 on page 35 to fill in the wizard fields.

3 Select the Next button to step through the wizard pages.

4 Confirm the configuration settings, and then select Finish and Close.

Note: If you change the IP address of the interface you are connecting to, you must connect through a web browser again using the new address. Browse to https:// followed by the new IP address of the interface. If the new IP address of the interface is on a different subnet, you may have to change the IP address of your computer to the same subnet.

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 example, for each server located on the Internal network the FortiGate unit adds an External->Internal firewall policy.

You are now finished the initial configuration of the FortiGate unit.

Connecting the FortiGate unit to the network(s)

After you complete the initial configuration, you can connect the FortiGate unit between the internal network and the Internet. You can also connect networks to the user-defined interfaces that you configured.

FortiGate-800

There are 4 10/100/1000 Base-TX connectors on the FortiGate-800:

- Internal for connecting to the internal network,
- External for connecting to your public switch or router and the Internet,
- DMZ for connecting to a DMZ network,
- HA for connecting to another FortiGate-800 for high availability (see "High availability installation" on page 51),

There are 4 10/100 Base-TX connectors on the FortiGate-800:

- user-defined interfaces 1 to 4 for connecting up to four additional networks to the FortiGate unit.

FortiGate-800F

There are 4 LC-SFP 1000Base-SX fiber transceivers on the FortiGate-800F:

- Internal for connecting to the internal network,
- External for connecting to your public switch or router and the Internet,
- DMZ for connecting to a DMZ network,
- HA for connecting to another FortiGate-800F for high availability (see "High availability installation" on page 51),

There are 4 10/100 Base-TX connectors on the FortiGate-800F:

- user-defined interfaces 1 to 4 for connecting up to four additional networks to the FortiGate unit.

Note: You can also create redundant connections to the Internet by connecting two interfaces to separate Internet connections. For example, you could connect the external interface and the DMZ interface or any available user-defined interface to different Internet connections, each provided by a different service provider.

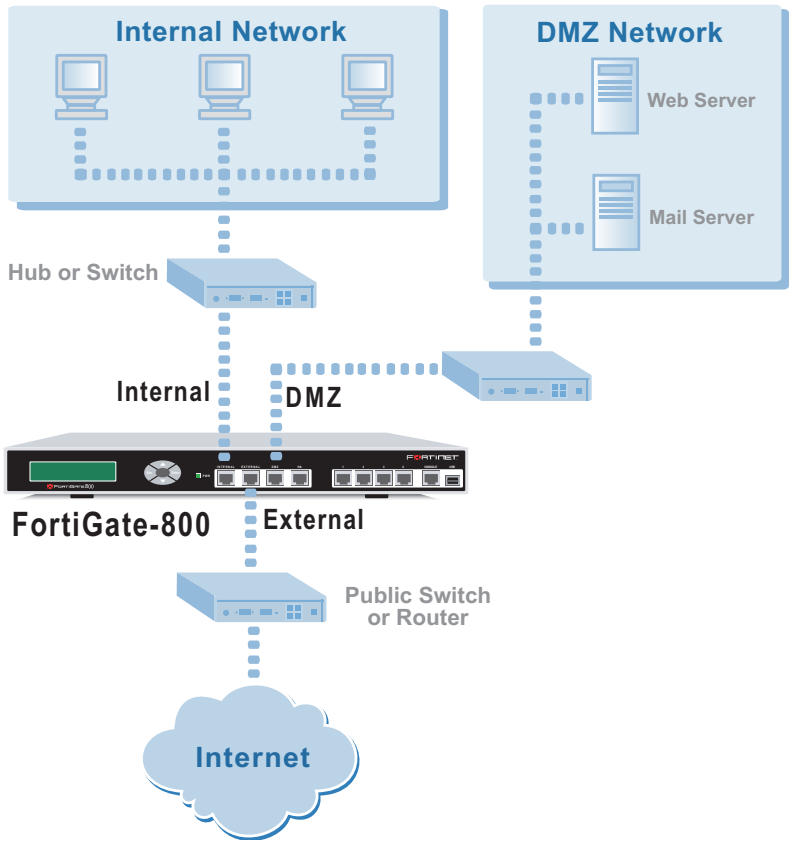
To connect the FortiGate unit running in NAT/Route mode

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

2 Connect the External interface to your public switch or router.

3 Optionally, connect the DMZ interface to the DMZ network.
You can use a DMZ network to provide access from the Internet to a web server or other server without installing the servers on the internal network.

Figure 10: FortiGate-800/800F NAT/Route mode connections



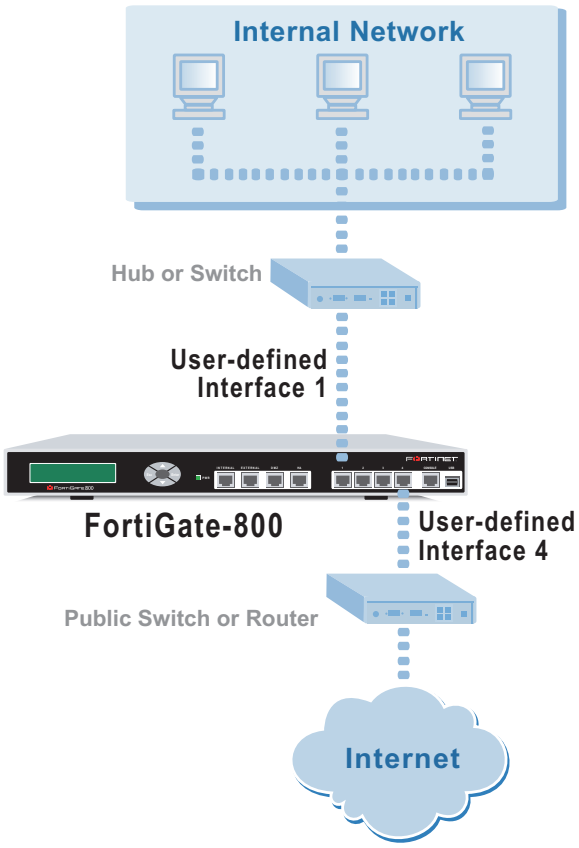
To connect to FortiGate-800/800F user-defined interfaces

1 Connect the user-defined interface to the hub or switch connected to the intended network.

2 Repeat for all user-defined interfaces that you have configured.

The example in Figure 11 shows an internal network connected to user-defined interface 1 and an external network connected to user-defined interface 4.

Figure 11: Example FortiGate-800/800F user-defined interface connections



Configuring the networks

If you are running the FortiGate unit in NAT/Route mode, the networks must be configured to route all Internet traffic to the IP address of the FortiGate interface to which they are connected.

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 the internal network. You should be able to connect to any Internet address.

In NAT/Route mode, you use the modem interface as either a backup interface or standalone interface to the Internet.

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.

The modem interface connected to the FortiGate USB interface. You must connect an external modem to the USB interface.

Next steps

You can use the following information to configure FortiGate system time, to register the FortiGate unit, and to configure antivirus and attack definition updates.

Refer to the *FortiGate Administration Guide* for complete information on configuring, monitoring, and maintaining the FortiGate unit.

To set the date and time

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

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

To use NTP to set the FortiGate date and time

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

To register the FortiGate unit

After purchasing and installing a new FortiGate unit, you can register the unit by going to the System Update Support page, or using a web browser to connect to http://support.fortinet.com and selecting Product Registration.

To register, enter your contact information and the serial numbers of the FortiGate units that you or your organization have purchased. You can register multiple FortiGate units in a single session without re-entering your contact information.

To configure virus, attack, and spam definition updates

You can configure the FortiGate unit to automatically keep virus, grayware, and attack definitions up to date.

1. Go to **System > Maintenance > Update Center**.
2. Select Refresh to test the FortiGate unit connectivity with the FortiProtect Distribution Network (FDN).

   To be able to connect to the FDN the FortiGate unit default route must point to a network such as the Internet to which a connection to the FDN can be established.

   If FortiProtect Distribution Network changes to Available, then the FortiGate unit can connect to the FDN.
3. Select Scheduled Update and configure a schedule for receiving antivirus and attack definition updates.
4. Select Apply.
5. You can also select Update Now to receive the latest virus and attack definition updates.

   For more information about FortiGate settings see the FortiGate Online Help or the *FortiGate Administration Guide*.

Transparent mode installation

This chapter describes how to install a FortiGate unit in Transparent mode. If you want to install the FortiGate unit in NAT/Route mode, see “NAT/Route mode installation” on page 27. If you want to install two or more FortiGate units in HA mode, see “High availability installation” on page 51. For more information about installing the FortiGate unit in Transparent mode, see “Planning the FortiGate configuration” on page 23.

This chapter describes:

Preparing to configure Transparent mode

Use Table 9 to gather the information that you need to customize Transparent mode settings.

You can configure Transparent mode using four methods:

- the web-based manager GUI
- front control buttons and LCD
- command line interface (CLI)
- setup wizard

The method you choose depends on the complexity of the configuration, access and equipment, and the type of interface you are most comfortable using.

Table 9: 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 web-based manager

You can use the web-based manager to complete the initial configuration of the FortiGate unit. You can continue to use the web-based manager for all FortiGate unit settings.

For information about connecting to the web-based manager, see “Connecting to the web-based manager” on page 16.

The first time 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 beside the Operation Mode.

3 Select Transparent in the Operation Mode list.

4 Select OK.

To reconnect to the web-based manager, change the IP address of the 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.

To change the Management IP

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

2 Enter the management IP address and netmask that you recorded in Table 9 on page 42.

3 Select access methods and logging for any interfaces as required.

4 Select Apply.

To configure DNS server settings

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

2 Enter the IP address of the primary DNS server.

3 Enter the IP address of the secondary DNS server.

4 Select OK.

To configure the default gateway

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

2 Set Default Gateway to the default gateway IP address that you recorded in Table 9 on page 42.

3 Select Apply.

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 front control buttons and LCD

This procedure describes how to use the control buttons and LCD to configure Transparent mode IP addresses. Use the information that you recorded in Table 9 on page 42 to complete this procedure. Starting with Main Menu displayed on the LCD, use the front control buttons and LCD:

To change the management IP address and netmask

1 Press Enter to display the option list.

2 Use the up and down arrows to highlight Manager interface.

3 Set the management interface IP address.

Use the up and down arrow keys to increase or decrease the value of each IP address digit. Press Enter to move to the next digit. Press Esc to move to the previous digit.

Note: When you enter an IP address, the LCD always shows three digits for each part of the address. For example, the IP address 192.168.100.1 appears on the LCD as 192.168.100.001. The IP address 192.168.23.45 appears as 192.168.023.045.

4 After you set the last digit of the IP address, press Enter.

5 Use the down arrow to highlight Netmask.

6 Press Enter and set the management IP Netmask.

7 After you set the last digit of the Netmask, press Enter.

8 Press Esc to return to the Main Menu.

To add a default gateway

1 Press Enter to display the option list.
2 Use the down arrow to highlight Default Gateway.
3 Press Enter and set the default gateway.
4 After you set the last digit of the default gateway, press Enter.
5 Press Esc to return to the Main Menu.

You have now completed the initial configuration of the FortiGate unit and you can proceed to "Next steps" on page 48.

Using the command line interface

As an alternative to the web-based manager or setup wizard you can begin the initial configuration of the FortiGate unit using the command line interface (CLI). To connect to the CLI, see "Connecting to the command line interface (CLI)" on page 17. Use the information that you gathered in Table 9 on page 42 to complete the following procedures.

To change to Transparent mode using the CLI

1 Make sure that you are logged into the CLI.
2 Switch to Transparent mode. Enter:

```
config system global
    set opmode transparent
  end
```

The FortiGate unit restarts. After a few seconds, the login prompt appears.

3 Type `admin` and press Enter.
The following prompt appears:

```
Welcome !
```

4 Confirm that the FortiGate unit has switched to Transparent mode. Enter:

```
get system status
```

The CLI displays the status of the FortiGate unit including the following line of text:

```
Operation mode: Transparent
```

To configure the management IP address

1 Make sure that you are logged into the CLI.
2 Set the management IP address and netmask to the IP address and netmask that you recorded in Table 9 on page 42. Enter:

```
config system manageip
    set ip <address_ip> <netmask>
  end
```

Example

```
config system manageip
    set ip 10.10.10.2 255.255.255.0
  end
```

3 Confirm that the address is correct. Enter:

```
get system manageip
```

The CLI lists the management IP address and netmask.

To configure DNS server settings

1 Set the primary and secondary DNS server IP addresses. Enter

```
config system dns
    set primary <address_ip>
    set secondary <address_ip>
  end
```

Example

```
config system dns
    set primary 293.44.75.21
    set secondary 293.44.75.22
  end
```

To configure the default gateway

1 Make sure that you are logged into the CLI.

2 Set the default route to the default gateway that you recorded in Table 9 on page 42. Enter:

```
config router static
    edit 1
        set dst 0.0.0.0 0.0.0.0
        set gateway <address_gateway>
        set device <interface>
  end
```

Example

If the default gateway IP is 204.23.1.2 and this gateway is connected to port 2:

```
config router static
    edit 1
        set dst 0.0.0.0 0.0.0.0
        set gateway 204.23.1.2
        set device port2
  end
```

Using the setup wizard

From the web-based manager, you can use the setup wizard to begin the initial configuration of the FortiGate unit. For information about connecting to the web-based manager, see “Connecting to the web-based manager” on page 16.

The first time 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 beside the Operation Mode.
3 Select Transparent in the Operation Mode list.
4 Select OK.

To reconnect to the web-based manager, change the IP address of the 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.

To start 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 9 on page 42 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.

Connecting the FortiGate unit to your network

After you complete the initial configuration of the FortiGate-800/800F unit, you can connect the FortiGate-800/800F between your internal network and the Internet and to other networks.

FortiGate-800

There are 4 10/100/1000 Base-TX connectors on the FortiGate-800:

- Internal for connecting to the internal network,
- External for connecting to your public switch or router and the Internet,
- DMZ for connecting to a DMZ network,
- HA for connecting to another FortiGate-800 for high availability (see “High availability installation” on page 51),

There are 4 10/100 Base-TX connectors on the FortiGate-800:

- user-defined interfaces 1 to 4 for connecting up to four additional networks to the FortiGate unit.

FortiGate-800F

There are 4 LC-SFP 1000Base-SX fiber transceivers on the FortiGate-800F:

- Internal for connecting to the internal network,
- External for connecting to your public switch or router and the Internet,
- DMZ for connecting to a DMZ network,
- HA for connecting to another FortiGate-800F for high availability (see "High availability installation" on page 51),

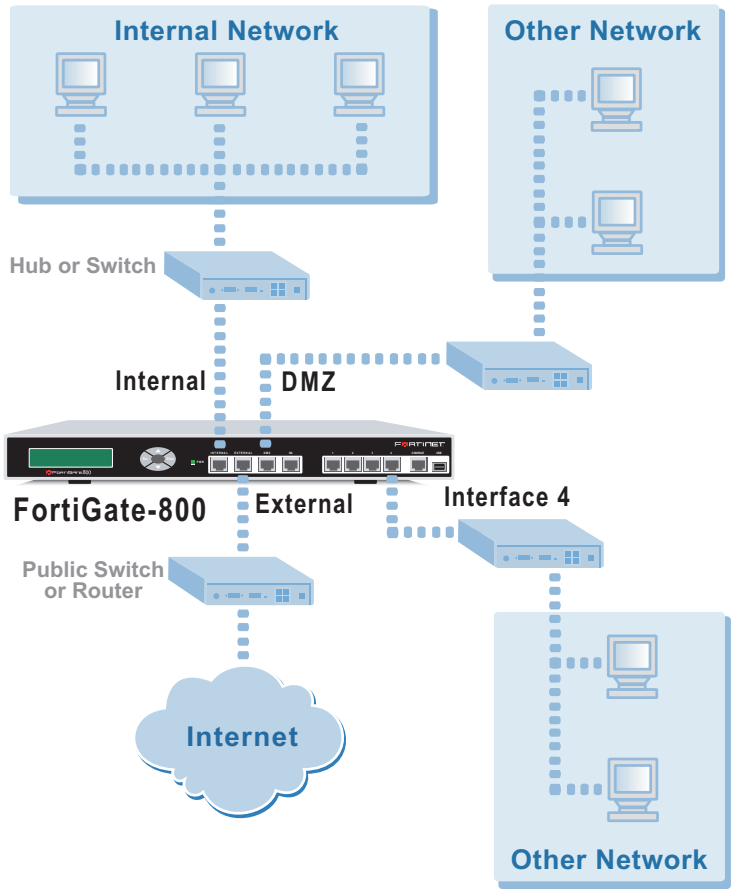
There are 4 10/100 Base-TX connectors on the FortiGate-800F:

- user-defined interfaces 1 to 4 for connecting up to four additional networks to the FortiGate unit.

To connect the FortiGate-800/800F unit running in Transparent mode:

1. Connect the Internal interface to the hub or switch connected to your internal network.
2. Connect the External interface to the network segment connected to the external firewall or router.
3. Optionally connect the DMZ and HA interfaces and interfaces 1 to 4 to hubs or switches connected to your other networks.

Figure 12: FortiGate-800/800F Transparent mode connections



Next steps

You can use the following information to configure FortiGate system time, to register the FortiGate unit, and to configure antivirus and attack definition updates.

Refer to the *FortiGate Administration Guide* for complete information on configuring, monitoring, and maintaining your FortiGate unit.

To set the date and time

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

1. Go to **System > Config > Time**.
2. Select Refresh to display the current FortiGate system date and time.
3. Select your Time Zone from the list.
4. Optionally, select Automatically adjust clock for daylight saving changes check box.

5 Select Set Time and set the FortiGate system date and time.

6 Set the hour, minute, second, month, day, and year as required.

7 Select Apply.

To use NTP to set the FortiGate date and time

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

2 Select Synchronize with NTP Server to configure the FortiGate unit to use NTP to automatically set the system time and date.

3 Enter the IP address or domain name of the NTP server that the FortiGate unit can use to set its time and date.

4 Specify how often the FortiGate unit should synchronize its time with the NTP server.

5 Select Apply.

To register your FortiGate unit

After purchasing and installing a new FortiGate unit, you can register the unit by going to the System Update Support page, or using a web browser to connect to http://support.fortinet.com and selecting Product Registration.

To register, enter your contact information and the serial numbers of the FortiGate units that you or your organization have purchased. You can register multiple FortiGate units in a single session without re-entering your contact information.

To configure virus, attack, and spam definition updates

You can configure the FortiGate unit to automatically keep virus, grayware, and attack definitions up to date.

1 Go to **System > Maintenance > Update Center**.

2 Select Refresh to test the FortiGate unit connectivity with the FortiProtect Distribution Network (FDN).

To be able to connect to the FDN the FortiGate unit default route must point to a network such as the Internet to which a connection to the FDN can be established.

If FortiProtect Distribution Network changes to Available, then the FortiGate unit can connect to the FDN.

3 Select Scheduled Update and configure a schedule for receiving antivirus and attack definition updates.

4 Select Apply.

5 You can also select Update Now to receive the latest virus and attack definition updates.

High availability installation

This chapter describes how to install two or more FortiGate units in an HA cluster. HA installation involves three basic steps:

- Configuring FortiGate units for HA operation
- Connecting the cluster to your networks
- Installing and configuring the cluster

For information about HA, see the *FortiGate Administration Guide* and the *FortiOS High Availability technical note*.

Priorities of heartbeat device and monitor priorities

The procedures in this chapter do not include steps for changing the priorities of heartbeat devices or for configuring monitor priorities settings. Both of these HA settings should be configured after the cluster is up and running.

Configuring FortiGate units for HA operation

A FortiGate HA cluster consists of two or more FortiGate units with the same HA configuration. This section describes how to configure each of the FortiGate units to be added to a cluster for HA operation. The procedures are the same for active-active and active-passive HA.

- High availability configuration settings
- Configuring FortiGate units for HA using the web-based manager
- Configuring FortiGate units for HA using the CLI

High availability configuration settings

Use the following table to select the HA configuration settings for the FortiGate units in the HA cluster.

Table 10: High availability settings

<table>
<tr><td rowspan="3">Mode</td><td>Active-Active</td><td>Load balancing and failover HA. Each FortiGate unit in the HA cluster actively processes connections and monitors the status of the other FortiGate units in the cluster. The primary FortiGate unit in the cluster controls load balancing.</td></tr>
<tr><td>Active-Passive</td><td>Failover HA. The primary FortiGate unit in the cluster processes all connections. All other FortiGate units in the cluster are passively monitor the cluster status and remain synchronized with the primary FortiGate unit.</td></tr>
<tr><td colspan="2">All members of the HA cluster must be set to the same HA mode.</td></tr>
<tr><td rowspan="11">Group ID</td><td colspan="2">The group ID range is from 0 to 63. All members of the HA cluster must have the same group ID.
When the FortiGate units in the cluster are switched to HA mode, all of the interfaces of all of the units in the cluster get the same virtual MAC address. This virtual MAC address is set according to the group ID.</td></tr>
<tr><td>Group ID</td><td>MAC Address</td></tr>
<tr><td>0</td><td>00-09-0f-06-ff-00</td></tr>
<tr><td>1</td><td>00-09-0f-06-ff-01</td></tr>
<tr><td>2</td><td>00-09-0f-06-ff-02</td></tr>
<tr><td>3</td><td>00-09-0f-06-ff-03</td></tr>
<tr><td>…</td><td></td></tr>
<tr><td>63</td><td>00-09-0f-06-ff-3f</td></tr>
<tr><td colspan="2">If you have more than one HA cluster on the same network, each cluster should have a different group ID. If two clusters on the same network have same group ID, the duplicate MAC addresses cause addressing conflicts on the network.</td></tr>
<tr><td>Unit priority</td><td colspan="2">The unit with the highest priority becomes the primary unit in the cluster. The unit priority range is 0 to 255. The default unit priority is 128.
Set the unit priority to a higher value if you want the FortiGate unit to be the primary cluster unit. Set the unit priority to a lower value if you want the FortiGate unit to be a subordinate unit in the cluster. If all units have the same priority, the FortiGate unit with the highest serial number becomes the primary cluster unit.</td></tr>
<tr><td>Override Master</td><td colspan="2">You can configure a FortiGate unit to always become the primary unit in the cluster by giving it a high priority and by selecting Override master.</td></tr>
</table>

Table 10: High availability settings (Continued)

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

Configuring FortiGate units for HA using the web-based manager

Use the following procedure to configure each FortiGate unit for HA operation.

To change the FortiGate unit host name

Changing the host name is optional, but you can use host names to identify individual cluster units.

1. Power on the FortiGate unit to be configured.
2. Connect to the web-based manager.
   See “Connecting to the web-based manager” on page 16.
3. Go to **System > Status**.
4. In the Host Name field of the Unit Information section, select Change.
5. Type a new host name and select OK.

To configure a FortiGate unit for HA operation

1. Go to **System > Config > HA**.
2. Select High Availability.
3. Select the mode.
4. Select a Group ID for the HA cluster.
5. If required, change the Unit Priority.
6. If required, select Override master.
7. Enter and confirm a password for the HA cluster.
8. If you are configuring Active-Active HA, select a schedule.
9. Select Apply.
   The FortiGate unit negotiates to establish an HA cluster. When you select apply you may temporarily lose connectivity with the FortiGate unit as the negotiation takes place.
10. If you are configuring a NAT/Route mode cluster, power off the FortiGate unit and then repeat this procedure for all the FortiGate units in the cluster. Once all of the units are configured, continue with "Connecting the cluster to your networks" on page 55.
11. If you are configuring a Transparent mode cluster, reconnect to the web-based manager.
    You may have to wait a few minutes before you can reconnect.
12. Go to **System > Status**.
13. Select Change to Transparent Mode and select OK to switch the FortiGate unit to Transparent mode.
14. Allow the FortiGate unit to restart in Transparent mode and then power off the FortiGate unit.
15. Repeat this procedure for all of the FortiGate units in the cluster.
16. Once all units are configured, continue with "Connecting the cluster to your networks" on page 55.

Configuring FortiGate units for HA using the CLI

Use the following procedure to configure each FortiGate unit for HA operation.

To change the FortiGate unit host name

1. Power on the FortiGate unit to be configured.
2. Connect to the CLI.
   See "Connecting to the command line interface (CLI)" on page 17.
3. Change the host name.

```
config system global
    set hostname <name_str>
  end
```

To configure the FortiGate unit for HA operation

1 Configure HA settings.

Use the following command to:

- Set the HA mode
- Set the Group ID
- Change the unit priority
- Enable override master
- Enter an HA password
- Select an active-active HA schedule

```
config system ha
    set mode {a-a | a-p | standalone}
    set groupid <id_integer>
    set priority <priority_integer>
    set override {disable | enable}
    set password <password_str>
    set schedule {hub | ip | ipport | leastconnection | none
  | random | round-robin | weight-round-robin}
  end
```

The FortiGate unit negotiates to establish an HA cluster.

2 If you are configuring a NAT/Route mode cluster, power off the FortiGate unit and then repeat this procedure for all the FortiGate units in the cluster. Once all of the units are configured, continue with "Connecting the cluster to your networks" on page 55.

3 If you are configuring a Transparent mode cluster, switch the FortiGate unit to Transparent mode.

```
config system global
    set opmode transparent
  end
```

4 Allow the FortiGate unit to restart in Transparent mode and then power off the FortiGate unit.

5 Repeat this procedure for all of the FortiGate units in the cluster then continue with "Connecting the cluster to your networks" on page 55.

Connecting the cluster to your networks

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

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

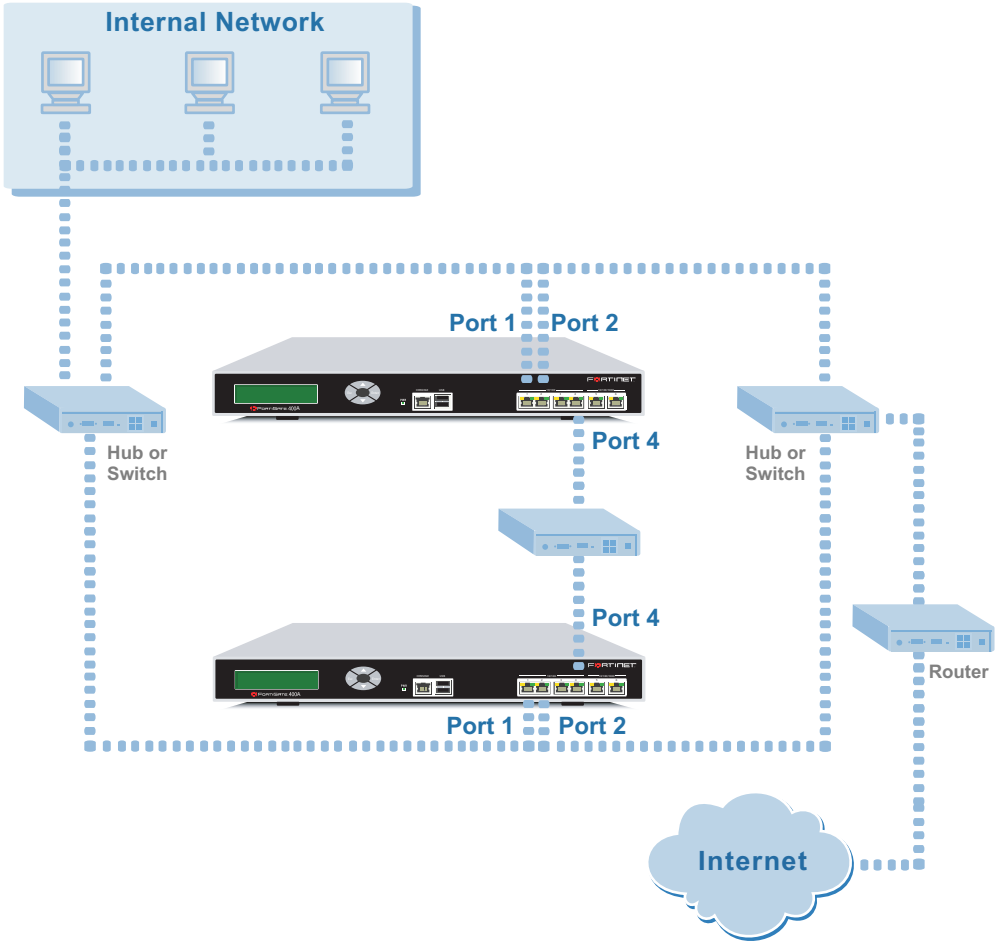
Inserting an HA cluster into your network temporarily interrupts communications on the network because new physical connections are being made to route traffic through the cluster. Also, starting the cluster interrupts network traffic until the individual FortiGate units in the cluster are functioning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

To connect the cluster

1 Connect the cluster units:

- Connect the internal interfaces of each FortiGate unit to a switch or hub connected to your internal network.
- Connect the external interfaces of each FortiGate unit to a switch or hub connected to your external network.
- Optionally connect the DMZ interfaces of each FortiGate unit to a switch or hub connected to your DMZ network.
- Optionally connect ports 1 to 4 of each FortiGate unit to switches or hubs connected to other networks.
- Connect the HA interfaces of the FortiGate units to another switch or hub. By default the HA interfaces are used for HA heartbeat communication. These interfaces should be connected together for the HA cluster to function.

Figure 13: HA network configuration



2 Power on all the FortiGate units in the cluster.

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

Installing and configuring the cluster

When negotiation is complete the you can configure the cluster as if it was a single FortiGate unit.

- If you are installing a NAT/Route mode cluster, use the information in "NAT/Route mode installation" on page 27 to install the cluster on your network
- If you are installing a Transparent mode cluster, use the information in "Transparent mode installation" on page 41 to install the cluster on your network.

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

When you connect to the cluster, you are actually connecting to the primary cluster unit. The cluster automatically synchronizes all configuration changes to the subordinate units in the cluster as the changes are made.

The only configuration settings that are not synchronized are the HA configuration (except for the interface heartbeat device and monitoring configuration) and the FortiGate host name.

For more information about configuring a cluster, see the *FortiGate Administration Guide*.

Index