INSTALL GUIDE

FortiGate-60/60M/ ADSL, FortiWiFi-60, and FortiGate-100A Version 3.0MR1

FORTINET™

www.fortinet.com

FortiGate-60 series and FortiGate-100A Install Guide
Version 3.0MR1
10 April 2006
01-30001-0266-20060410

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

⚠ **Caution:** If you install a battery that is not the correct type, it could explode. Dispose of used batteries according to local regulations.

Contents

Introduction

Welcome and thank you for selecting Fortinet products for your real-time network protection.

The FortiGate™ Unified Threat Management System improves network security, reduces network misuse and abuse, and helps you use communications resources more efficiently without compromising the performance of your network. FortiGate Unified Threat Management Systems are ICSA-certified for firewall, IPSec, and antivirus services.

The FortiGate Unified Threat Management System is a dedicated, easily managed security device that delivers a full suite of capabilities, which 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 Unified Threat Management System uses Fortinet's Dynamic Threat Prevention System (DTPS™) 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.

Fortinet Family Products

Fortinet offers a family of products that includes both software and hardware appliances, for a complete network security solution including mail, logging, reporting, network management, and security along with FortiGate Unified Threat Management Systems. For more information on the Fortinet product family, go to www.fortinet.com/products.

FortiGuard Subscription Services

FortiGuard Subscription Services are security services created, updated and managed by a global team of Fortinet security professionals. They ensure the latest attacks are detected and blocked before harming your corporate resources or infecting your end-user computing devices. These services are created with the latest security technology and designed to operate with the lowest possible operational costs.

FortiGuard Subscription Services includes:

- FortiGuard Antivirus Service
- FortiGuard Intrusion Prevention subscription services (IPS)

- FortiGuard Web Filtering
- FortiGuard Antispam Service
- FortiGuard Premier Service

An online virus scanner and virus encyclopedia is also available for your reference.

FortiClient

FortiClient™ Host Security software provides a secure computing environment for both desktop and laptop users running the most popular Microsoft Windows operating systems. FortiClient offers many features including:

- creating VPN connections to remote networks
- configuring real-time protection against viruses
- guarding against modification of the Windows registry
- virus scanning

FortiClient also offers a silent installation feature, enabling an administrator to efficiently distribute FortiClient to several users' computers with preconfigured settings.

FortiMail

FortiMail™ Secure Messaging Platform provides powerful, flexible heuristic scanning and reporting capabilities to incoming and outgoing email traffic. The FortiMail unit has reliable, high performance features for detecting and blocking malicious attachments such as Distributed Checksum Clearinghouse (DCC) scanning and Bayesian scanning. Built on Fortinet's award winning FortiOS and FortiASIC technology, FortiMail antivirus technology extends full content inspection capabilities to detect the most advanced email threats.

FortiAnalyzer

FortiAnalyzer™ provides network administrators with the information they need to enable the best protection and security for their networks against attacks and vulnerabilities. The FortiAnalyzer unit features include:

- collects logs from FortiGate devices and syslog devices
- creates hundreds of logs using collected log data
- scans and reports vulnerabilities
- stores files quarantined from a FortiGate unit

The FortiAnalyzer unit can also be configured as a network analyzer to capture real-time traffic on areas of your network where firewalls are not employed. You can also use the unit as a storage device where users can access and share files, including the reports and logs that are saved on the FortiAnalyzer hard disk.

FortiReporter

FortiReporter™ Security Analyzer software generates easy-to-understand reports and can collect logs from any FortiGate unit, as well as over 30 network and security devices from third-party vendors. FortiReporter reveals network abuse, manages bandwidth requirements, monitors web usage, and ensures employees are using the office network appropriately. FortiReporter allows IT administrators to identify and respond to attacks, including identifying ways to proactively secure their networks before security threats arise.

FortiBridge

FortiBridge™ products are designed to provide enterprise organizations with continuous network traffic flow in the event of a power outage or a FortiGate system failure. The FortiBridge unit bypasses the FortiGate unit to make sure that the network can continue processing traffic. FortiBridge products are easy to use and deploy, and you can customize the actions a FortiBridge unit takes when a power failure or a FortiGate system failure occurs.

FortiManager

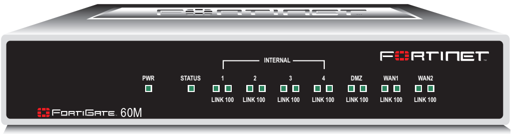
The FortiManager™ system is designed to meet the needs of large enterprises (including managed security service providers) responsible for establishing and maintaining security policies across many dispersed FortiGate installations. With this system, you can configure multiple FortiGate devices and monitor their status. You can also view real-time and historical logs for the FortiGate devices, including updating firmware images of managed FortiGate devices. The FortiManager System emphasizes ease of use, including easy integration with third party systems.

About the FortiGate unit

The FortiGate-60 series and FortiGate-100A appliances are designed for small businesses (including telecommuters), to deliver the same enterprise-class network-based antivirus, content filtering, firewall, VPN, and network-based intrusion detection/prevention featured in all FortiGate units. The FortiGate-60 series and FortiGate-100A also feature High Availability (HA) support.

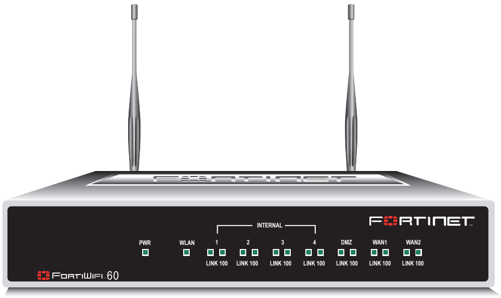
FortiGate-60/60M/ADSL

The FortiGate-60 unit is designed for telecommuters remote offices, and retail stores. The FortiGate-60 unit includes an external modem port that can be used as a backup or stand alone connection to the Internet while the FortiGate-60M unit includes an internal modem that can also be used either as a backup or a standalone connection to the Internet. The FortiGate-60ADSL includes an internal ADSL modem.



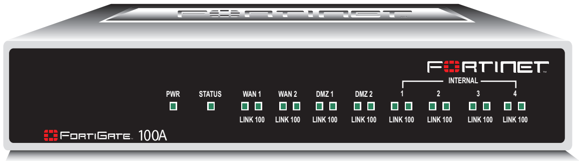
FortiWiFi-60

The FortiWiFi-60 model provides a secure, wireless LAN solution for wireless connections. It combines mobility and flexibility with FortiWiFi Antivirus Firewall features, and can be upgraded to future radio technologies. The FortiWiFi-60 serves as the connection point between wireless and wired networks or the center-point of a standalone wireless network.



FortiGate-100A

The FortiGate-100A unit is designed to be an easy-to-administer solution for small offices, home offices, and branch office applications.



The FortiGate-100A supports advanced features such as 802.1Q VLAN, virtual domains, and the RIP and OSPF routing protocols.

About this document

This document explains how to install and configure your FortiGate unit onto your network. This document also includes how to install and upgrade new firmware versions on your FortiGate unit.

This document contains the following chapters:

- Installing the FortiGate unit – Describes setting up, and powering on a FortiGate unit.
- Factory defaults – Provides the factory default settings for the FortiGate unit.
- Configuring the FortiGate unit for the network – Provides an overview of the operating modes of the FortiGate unit and how to integrate the FortiGate unit into your network.
- Configuring the modem interface – Describes how to configure and use a modem with the FortiGate-60 series.
- Configuring the ADSL modem interface – Describes how to configure and use the ADSL modem available in the FortiGate-60ADSL.
- Using a wireless network – Outlines the considerations for wireless networking and steps you can take to make your wireless network as efficient as possible.
- FortiGate Firmware – Describes how to install, update, restore and test the firmware for the FortiGate device.

Note: This guide covers information on five FortiGate units; the FortiGate-60/60M, FortiWiFi-60, and FortiGate-100A. While most of the content applies to all the units, where information is specific to a certain model, an icon like the ones below will appear next to the content.

Document conventions

The following document conventions are used in this guide:

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

Note: Highlights useful additional information.

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

Typographic conventions

FortiGate documentation uses the following typographical conventions:

Convention	Example
Keyboard input	In the Gateway Name field, type a name for the remote VPN peer or client (for example, `Central_Office_1`).

Code examples	`config sys global`
	`    set ips-open enable`
	`  end`

CLI command syntax	`config firewall policy`
	`  edit id_integer`
	`    set http_retry_count <retry_integer>`
	`    set natip <address_ipv4mask>`
	`  end`

Document names	*FortiGate Administration Guide*
Menu commands	Go to **VPN > IPSEC > Phase 1** and select Create New.
Program output	`Welcome!`
Variables	`<address_ipv4>`

Fortinet documentation

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

The following FortiGate product documentation is available:

- *FortiGate QuickStart Guide*

  Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Install Guide*

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

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

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

  Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*

  Available exclusively from the Fortinet Knowledge Center, the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*

  Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*

  Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*

  Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*

  Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*

  Explains how to configure a PPTP VPN using the web-based manager.

- *FortiGate Certificate Management User Guide*

  Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*

  Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet Knowledge Center

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

Comments on Fortinet technical documentation

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

Customer service and technical support

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

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

Installing the FortiGate unit

This section provides information on installing and setting up the FortiGate unit on your network. This section includes the following topics:

- Package Contents
- Mounting
- Powering on the FortiGate unit
- Connecting to the FortiGate unit

Package Contents

Review the contents of your FortiGate package to ensure all components were included.

FortiGate-60/60M/ADSL

The FortiGate-60/60M/ADSL package each contain the following items:

- FortiGate-60 Unified Threat Management System
- one orange crossover Ethernet cable (Fortinet part number CC300248)
- one gray straight-through Ethernet cable (Fortinet part number CC300249)
- one RJ-45 to DB-9 serial cable (Fortinet part number CC300247)
- one RJ-11 phone cable (FortiGate-60M only)
- one power cable and one AC adapter
- FortiGate-60 QuickStart Guide, FortiGate-60M QuickStart Guide or FortiGate-60ADSL QuickStart Guide
- Fortinet Documentation CD

Figure 1: FortiGate-60/60M package contents

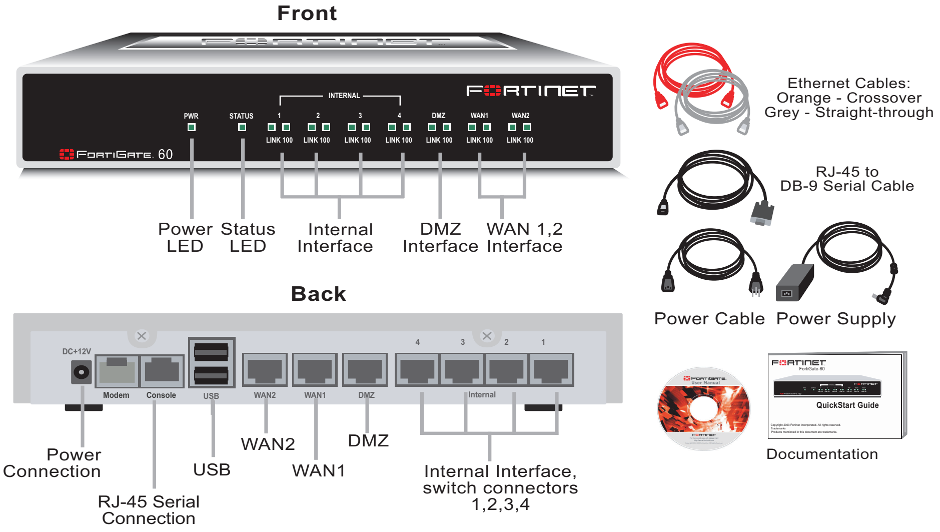


Table 1: Technical Specifications

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: 12V DC input current: 3A
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

FortiWiFi-60

The FortiWiFi-60 package contains the following items:

- FortiWiFi-60 Unified Threat Management System
- one orange crossover Ethernet cable (Fortinet part number CC300248)
- one gray straight-through Ethernet cable (Fortinet part number CC300249)
- one RJ-45 to DB-9 serial cable (Fortinet part number CC300247)
- one power cable and one AC adapter
- FortiWiFi-60 QuickStart Guide
- Fortinet Documentation CD

Figure 2: FortiWiFi-60 package contents

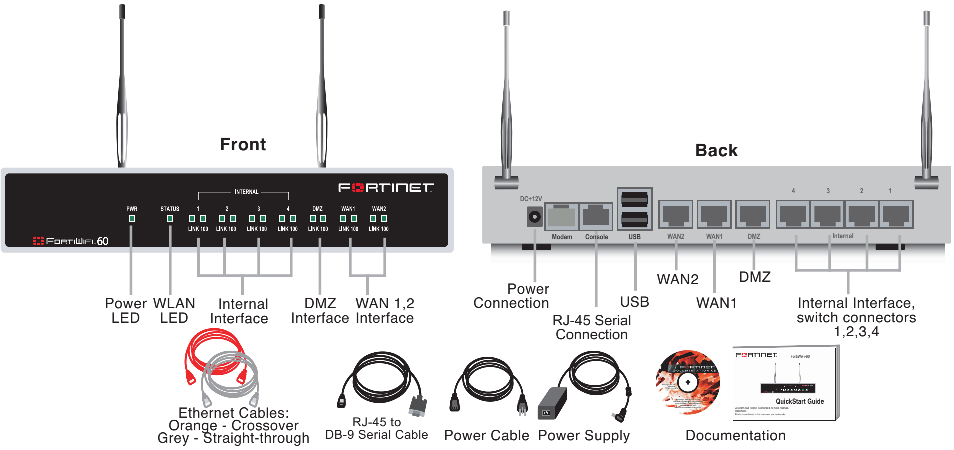


Table 2: Technical Specifications

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: 12V DC input current: 3A
Wireless Connectivity	Antenna type: Dual external fixed antenna Antenna range: 802.11 b/g:2.4GHz Antenna Gain: 5dBi
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

FortiGate-100A

The FortiGate-100A package contains the following items:

- FortiGate-100A Unified Threat Management System
- one orange crossover Ethernet cable (Fortinet part number CC300248)
- one gray straight-through Ethernet cable (Fortinet part number CC300249)
- one RJ-45 to DB-9 serial cable (Fortinet part number CC300302)
- one power cable and one AC adapter
- FortiGate-100A QuickStart Guide
- Fortinet Documentation CD

Figure 3: FortiGate-100A package contents

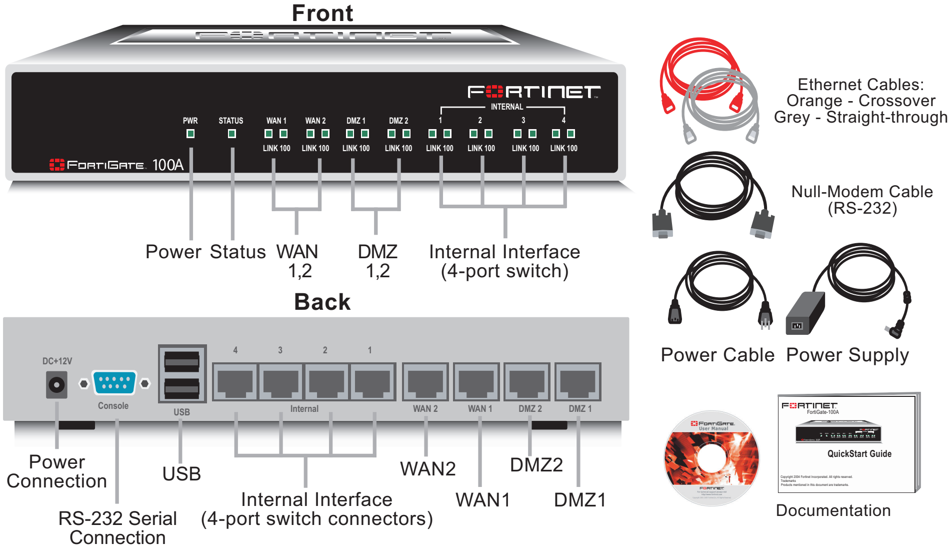


Table 3: Technical Specifications

Dimensions	10.25 x 6.13 x 1.75 in. (26 x 15.6 x 345 cm)
Weight	1.75 lb. (0.8 kg)
Power Requirements	DC input voltage: 12V DC input current: 5A
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

Mounting

Install the FortiGate unit on any stable, flat surface. Make sure the unit has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Powering on the FortiGate unit

The FortiGate unit does not have an on/off switch.

To power on the FortiGate unit

1 Connect the AC adapter to the power connection at the back of the FortiGate unit.

2 Connect the AC adapter to the power cable.

3 Connect the power cable to a power outlet.

The FortiGate unit starts and the Power and Status LEDs light up. The Status LEDs flash while the FortiGate unit starts up, and remain lit when the system is running.

Table 4: LED indicators

LED	State	Description
Power	Green	The FortiGate unit is powered on.
	Off	The FortiGate unit is powered off.
Status	Flashing	The FortiGate unit is starting up.
	Green	The FortiGate unit is running normally.
	Off	The FortiGate unit is powered off.
Link (Internal DMZ1 DMZ2 WAN 1 WAN 2)	Green	The correct cable is in use, and the connected equipment has power.
	Flashing green	Network activity at this interface.
	Off	No link established.
DMZ1 DMZ2 WAN 1 WAN 2	Green	The interface is connected at 100 Mbps.

Powering off the FortiGate unit

Always shut down the FortiGate operating system properly before unplugging the power to avoid potential hardware problems.

To power off the FortiGate unit

1 From the web-based manager, go to **System > Status > System Operation**, select Shutdown and then select Go, or from the CLI, enter:

```
execute shutdown
```

2 Disconnect the power supply.

Connecting to the FortiGate unit

There are two methods of connecting and configuring the basic FortiGate settings:

- the web-based manager
- the command line interface (CLI)

Web-based manager

You can configure and manage the FortiGate unit using HTTP or a secure HTTPS connection from any computer running Microsoft Internet Explorer 6.0 or recent browser. The web-based manager supports multiple languages.

You can use the web-based manager to configure most FortiGate settings, and monitor the status of the FortiGate unit.

Command line interface

You can access the FortiGate command line interface (CLI) by connecting a management computer serial port to the FortiGate 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.

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 require:

- a computer with an Ethernet connection
- Microsoft Internet Explorer version 6.0 or higher or any recent version of most popular web browser
- a crossover Ethernet cable or an Ethernet hub with two Ethernet cables

Note: Before starting Internet Explorer, (or any recent version of the most popular web browser), ping to your FortiGate unit to see if the connection between the computer and the FortiGate unit is working properly.

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.

You can also configure the management computer to obtain an IP address automatically using the 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.

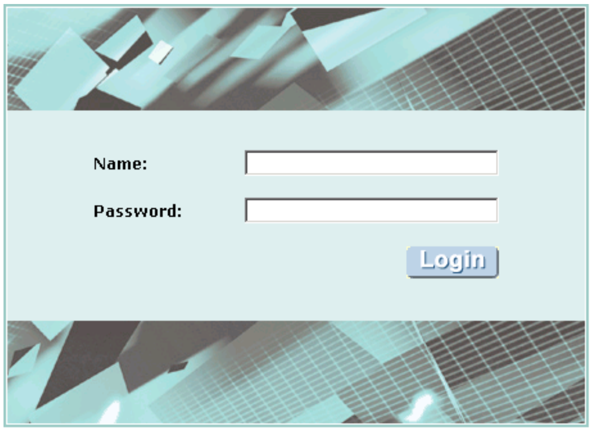
3 Start Internet Explorer and browse to the address https://192.168.1.99. (remember to include the “s” in https://).

To support a secure HTTPS authentication method, the FortiGate unit ships with a self-signed security certificate, and is offered to remote clients whenever they initiate a HTTPS connection to the FortiGate unit. When you connect, the FortiGate unit displays two security warnings in the browser.

The first warning prompts you to accept and optionally install the FortiGate unit's self-signed security certificate. If you do not accept the certificate, the FortiGate unit refuses the connection. If you accept the certificate, the FortiGate login page appears. The credentials entered are encrypted before they are sent to the FortiGate unit. If you choose to accept the certificate permanently, the warning is not displayed again.

Just before the FortiGate login page is displayed, a second warning informs you that the FortiGate certificate distinguished name differs from the original request. This warning occurs because the FortiGate unit redirects the connection. This is an informational message. Select OK to continue logging in.

Figure 4: FortiGate login

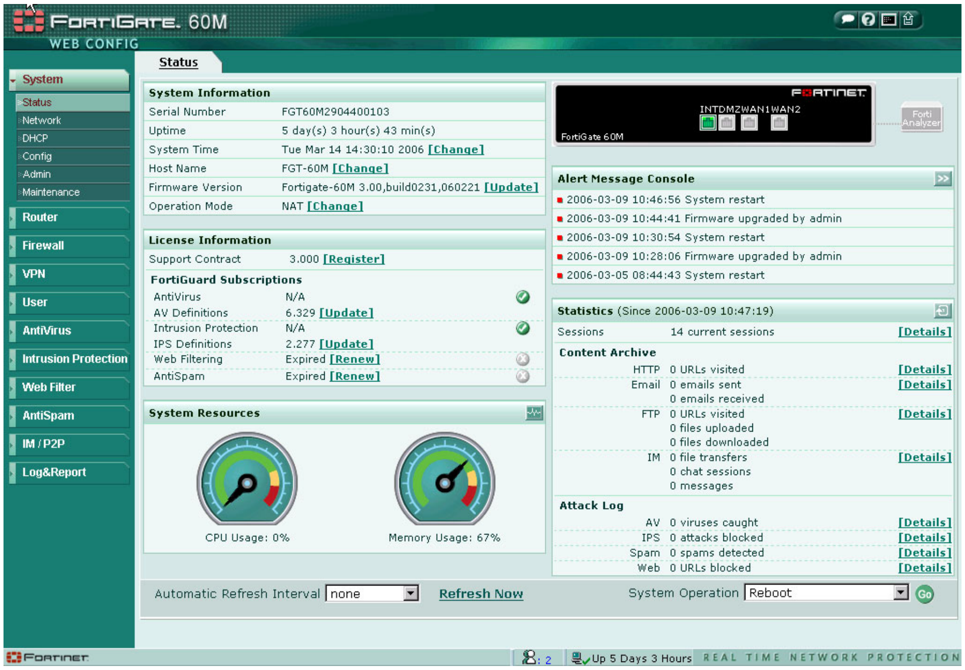


4 Type `admin` in the Name field and select Login.

System Dashboard

After logging into the web-based manager, the web browser displays the system dashboard. The dashboard provides you with all system status information in one location.

Figure 5: System dashboard for the FortiGate-60M



System Information

Serial Number	FGT60M2904400103
Uptime	5 day(s) 3 hour(s) 43 min(s)
System Time	Tue Mar 14 14:30:10 2006 [Change]
Host Name	FGT-60M [Change]
Firmware Version	Fortigate-60M 3.00,build0231,060221 [Update]
Operation Mode	NAT [Change]

License Information

Support Contract	3.000 [Register]	
FortiGuard Subscriptions		
AntiVirus	N/A	✓
AV Definitions	6.329 [Update]	
Intrusion Protection	N/A	✓
IPS Definitions	2.277 [Update]	
Web Filtering	Expired [Renew]	☒
AntiSpam	Expired [Renew]	☒

System Resources

CPU Usage: 0%

Memory Usage: 67%

Alert Message Console

- 2006-03-09 10:46:56 System restart
- 2006-03-09 10:44:41 Firmware upgraded by admin
- 2006-03-09 10:30:54 System restart
- 2006-03-09 10:28:06 Firmware upgraded by admin
- 2006-03-05 08:44:43 System restart

Statistics (Since 2006-03-09 10:47:19)

Sessions	14 current sessions	[Details]
Content Archive		
HTTP	0 URLs visited	[Details]
Email	0 emails sent 0 emails received	[Details]
FTP	0 URLs visited 0 files uploaded 0 files downloaded	[Details]
IM	0 file transfers 0 chat sessions 0 messages	[Details]
Attack Log		
AV	0 viruses caught	[Details]
IPS	0 attacks blocked	[Details]
Spam	0 spams detected	[Details]
Web	0 URLs blocked	[Details]

Automatic Refresh Interval: none   Refresh Now   System Operation: Reboot   Go

: 2   Up 5 Days 3 Hours

The dashboard includes the following information:

- Port Status – the dashboard includes an image of the front panel of the FortiGate unit. It also includes the FortiAnalyzer connection status—an X means there is no connection, and a check mark means there is a connection. The FortiLog unit will be gray unless the FortiGate unit is connected to a FortiLog unit. The port information is available by hovering your mouse over the port. The information includes whether the port is up or down, IP address and netmask, speed, and total sent and received packets. Each port appears green when the port is active.
- System information – displays the operating system information including the unit's serial number and firmware build. Use this area to update the firmware, set the system time or change the operating mode.
- System Resources – displays and enables you to monitor the use of resources for the unit. If you are connected to a FortiAnalyzer unit, the FortiAnalyzer unit's disk usage is also displayed.
- License Information – displays the current antivirus and security updates on your FortiGate unit.
- Alert Message Console – displays recent alert messages for events that have recently occurred on your FortiGate unit.
- Statistics – provides you with real-time information on the through traffic and attacks on your FortiGate unit.

Command line interface

You can access the FortiGate command line interface (CLI) by connecting a management computer serial port to the FortiGate 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 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*.

Connecting to the 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 require:

- a computer with an available communications port
- the RJ-45 to DB-9 serial cable included in your FortiGate package
- terminal emulation software such as HyperTerminal for Microsoft Windows

Note: The following procedure uses Microsoft Windows HyperTerminal software. You can apply these steps to any terminal emulation program.

To connect to the CLI

1 Connect the RJ-45 to DB-9 serial cable/console port.

2 Start HyperTerminal, enter a name for the connection and select OK.

3 Configure HyperTerminal to connect directly to the communications port on your computer and select OK.

4 Select the following port settings and select OK:

5 Press Enter to connect to the FortiGate CLI.

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

The login prompt appears.

6 Type `admin` and press Enter twice.

The following prompt is displayed:

```
Welcome !
```

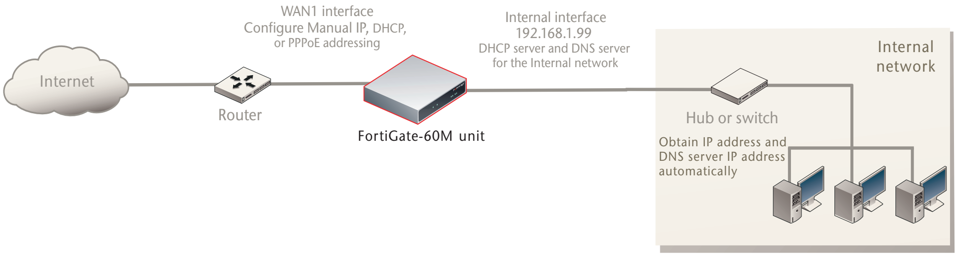
Type ? to list available commands. For information about how to use the CLI, see the *FortiGate CLI Reference*.

Quick installation using factory defaults

You can quickly set up your FortiGate-60 series unit for a home or small office using the web-based manager and the factory default FortiGate configuration. All you need to do is set your network computers to obtain an IP address automatically and to obtain DNS server IP addresses automatically (using DHCP), access the web-based manager, and configure the required settings for the FortiGate WAN1 interface. You can also configure FortiGate DNS servers and add a FortiGate default route if needed.

The FortiGate internal interface acts as a DHCP server for the internal network, automatically assigning IP addresses to computers (up to 100 computers) in the range of 192.168.1.110 –192.168.1.210.

Figure 6: Quick configuration using default settings


WAN1 interface
Configure Manual IP, DHCP, or PPPoE addressing
Internal interface
192.168.1.99
DHCP server and DNS server for the Internal network
Internal network
Internet
Router
FortiGate-60M unit
Hub or switch
Obtain IP address and DNS server IP address automatically

The FortiGate DHCP server also assigns the DNS server IP address 192.168.1.99 to each computer on the internal network. As a result, the FortiGate unit internal interface acts as a DNS server for the internal network. Using DNS forwarding, the FortiGate unit forwards DNS requests received from the internal network to the DNS server IP addresses added to the FortiGate unit configuration and returns lookup results to the internal network.

For more information about default DHCP server settings see “Factory default DHCP server configuration” on page 26.

The following procedure describes how to configure your internal network and the FortiGate unit to use the FortiGate default settings.

1 Connect the FortiGate unit between the internal network and the Internet and turn on the power.

2 Set the TCP/IP properties of the network computers to obtain an IP address automatically and a DNS server IP address automatically (using DHCP).

3 From the management computer, browse to https://192.168.1.99.

The FortiGate web-based manager appears.

4 Go to **System > Network > Interface** and select Edit for the external interface.

5 Select one of the following Addressing modes:

- Manual: enter a static IP address and netmask, select OK, and go to step 6
- DHCP: to get an IP address from the ISP select DHCP and go to step 9
- PPPoE: to get an IP address from the ISP select PPPoE and go to step 9

6 Go to **System > Network > Options**.

7 Select one of the following DNS settings:

- Obtain DNS server address automatically: select to get the DNS addresses from the ISP, select Apply
- Use the following DNS server addresses: select and enter the DNS server addresses given to you by the ISP, select Apply

8 Go to **Router > Static**, edit route #1 and change Gateway to the default gateway IP address from the ISP and select OK.

Network configuration is complete. Proceed to “Next steps” on page 45.

9 Select Retrieve default gateway from server and Override internal DNS options if your ISP supports them, select OK, and proceed to “Next steps” on page 45.
Go to step 6 if you are not selecting these options.

Factory defaults

The FortiGate unit ships 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, if required, configure basic routing.

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 you complete the network configuration, 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 firewall policies to provide more control of the network traffic passing through 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.

This section includes the following topics:

- Factory default DHCP server configuration
- Factory default NAT/Route mode network configuration
- Factory default Transparent mode network configuration
- Factory default firewall configuration
- Restoring the default settings

Factory default DHCP server configuration

Using the factory default DHCP server settings, you can quickly configure the internal network and the FortiGate unit. See “Quick installation using factory defaults” on page 23.

Table 5: Factory default DHCP server configuration

Name	internal_dhcp_server
Interface	Internal
Default Gateway	192.168.1.99
IP Range	192.168.1.110 – 192.168.1.210
Network Mask	255.255.255.0
Lease Duration	7 days
DNS Server 1	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 6 on page 26. 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 6 on page 26, 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 6: 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 HTTP, HTTPS, Ping
WAN1 interface	IP: Netmask: Administrative Access:	192.168.100.99 255.255.255.0 Ping
WAN2 interface	IP: Netmask: Administrative Access:	192.168.101.99 255.255.255.0 Ping
DMZ interface DMZ1 (FortiGate-100A)	IP: Netmask: Administrative Access:	10.10.10.1 255.255.255.0 HTTPS, Ping
DMZ2 interface (FortiGate-100A)	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0 Ping

Table 6: Factory default NAT/Route mode network configuration (Continued)

Modem interface	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0
ADSL Modem interface	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0
WLAN	IP: Netmask: Administrative Access:	10.10.80.1 255.255.255.0 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 Secondary DNS Server	65.39.139.53 65.39.139.63

Factory default Transparent mode network configuration

In Transparent mode, the FortiGate unit has the default network configuration listed in Table 7.

Table 7: Factory default Transparent mode network configuration

Administrator account	User name: Password:	admin (none)
Management IP	IP: Netmask:	0.0.0.0 0.0.0.0
DNS	Primary DNS Server: Secondary DNS Server:	65.39.139.53 65.39.139.63
Administrative access	Internal	HTTPS, Ping
	DMZ	HTTPS, Ping
	DMZ1	HTTPS, Ping
	DMZ2	Ping
	WAN1	Ping
	WAN2	Ping
	WLAN	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. The factory default configuration contains one firewall policy that allows all traffic originating on the internal network to access the Internet. No other traffic is allowed 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 8: Factory default firewall configuration

Configuration setting	Name	Description
Firewall policy	Internal -> External	Source: All Destination: All
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 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

By 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 and file quarantining 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 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.

Restoring the default settings

You can revert to factory default settings and start over again if you mistakenly change a network setting and are unable to recover from it.

⚠ **Caution:** This procedure deletes all changes you have made to the FortiGate configuration and reverses the system to its original configuration, including resetting interface addresses.

Restoring the default settings using the web-based manager

To reset the default settings

1. Go to **System > Status > System Operation**.
2. Select Reset to factory default.
3. Select Go.

Restoring the default settings using the CLI

To reset the default settings enter the following command:

```
execute factoryreset
```

Configuring the FortiGate unit for the network

This section provides an overview of the operating modes of the FortiGate unit. Before beginning to configure the FortiGate unit, you need to plan how to integrate the unit into your network. Your configuration plan depends on the operating mode you select: NAT/Route mode or Transparent mode.

This section includes the following topics:

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 you select. You can configure the FortiGate unit in one of two modes: NAT/Route mode (the default) or Transparent mode.

You can also configure the FortiGate unit and the network it protects using the default settings.

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:

Table 9: NAT/Route mode network segments

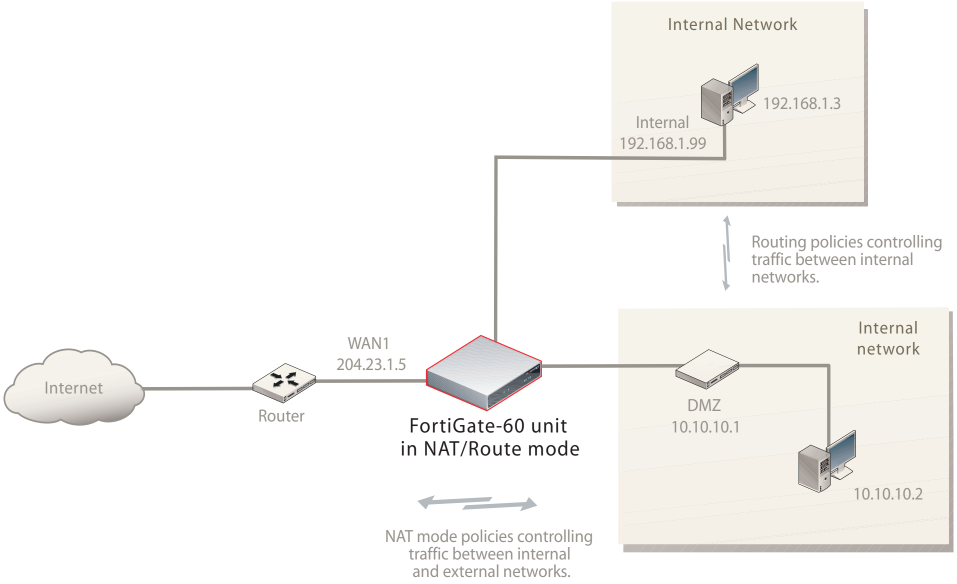
FortiGate Unit	Internal Interface	External Interface	Other
FortiGate-60	Internal (1, 2, 3, 4)	WAN1 WAN2	DMZ
FortiGate-60M	Internal	WAN1 WAN2	DMZ
FortiWiFi-60	Internal	WLAN	DMZ WAN1 WAN2
FortiGate-60ADSL	Internal	WAN1 WAN2	DMZ
FortiGate-100A	Internal	WAN1 WAN2	DMZ1 DMZ2

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).

Note: 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 mode network configuration for a FortiGate-60 unit.



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).

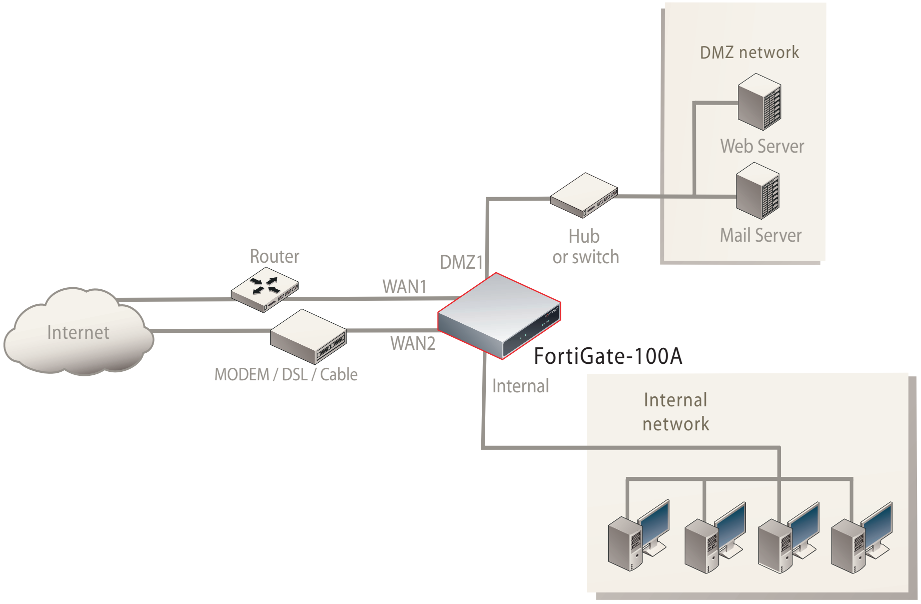
For example, you could create the following configuration:

- WAN1 is the default interface to the external network (usually the Internet)
- Modem is the redundant interface to the external network for the FortiGate-60 series
- DMZ is the redundant interface to the external network on the FortiGate-100A
- Internal is the interface to the internal network

You must configure routing to support redundant Internet connections. Routing can 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).

Figure 8: Example NAT/Route multiple internet connection configuration for a FortiGate-100A



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.

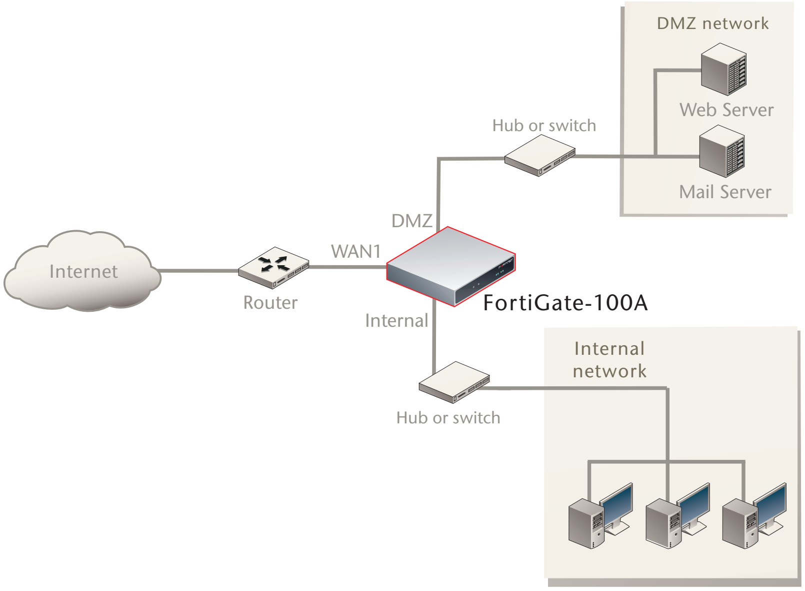
You can connect up to four network segments to the FortiGate unit to control traffic between these network segments.

Table 10: Transparent mode network segments

FortiGate Unit	Internal Interface	External Interface	Other
FortiGate-60	Internal (1, 2, 3, 4)	WAN1	WAN2 DMZ
FortiGate-60M	Internal	WAN1 WAN2	DMZ
FortiWiFi-60	Internal	WLAN	DMZ WAN1 WAN2
FortiGate-60ADSL	Internal	WAN1	WAN2 DMZ
FortiGate-100A	Internal	WAN1	WAN2 DMZ1 DMZ2

Note: In Transparent mode, the modem interface is not available on the FortiGate-60M.

Figure 9: Example Transparent mode network configuration for a FortiGate-100A.



Preventing the public FortiGate interface from responding to ping requests

The factory default configuration of your FortiGate unit allows the default public interface to respond to ping requests. The default public interface is also called the default external interface, and is the interface of the FortiGate unit that is usually connected to the Internet.

For the most secure operation, you should change the configuration of the external interface so that it does not respond to ping requests. Not responding to ping requests makes it more difficult for a potential attacker to detect your FortiGate unit from the Internet.

Depending on the FortiGate unit, the default public interface can be the external or WAN1 interface.

A FortiGate unit responds to ping requests if ping administrative access is enabled for that interface. You can use the following procedures to disable ping access for the external interface of a FortiGate unit. You can use the same procedure for any FortiGate interface. You can also use the same procedure in NAT/Route or Transparent mode.

To disable ping administrative access from the web-based manager

1 Log into the FortiGate web-based manager.

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

3 Choose the external interface and select Edit.

4 Clear the Ping Administrative Access check box.

5 Select OK to save the changes.

To disable ping administrative access from the FortiGate CLI

1 Log into the FortiGate CLI.

2 Disable administrative access to the external interface. Enter:

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

NAT/Route mode installation

This section describes how to install the FortiGate unit in NAT/Route mode. This section includes the following topics:

- Preparing to configure the FortiGate unit in NAT/Route mode
- DHCP or PPPoE configuration
- Using the web-based manager
- Using the command line interface
- Connecting the FortiGate unit to the network(s)
- Configuring the networks

Preparing to configure the FortiGate unit in NAT/Route mode

Use Table 11 on page 36 to gather the information you need to customize NAT/Route mode settings.

You can configure the FortiGate unit in two ways:

- The web-based manager GUI is a complete interface for configuring most settings. See “Using the web-based manager” on page 37.
- The command line interface (CLI) is a complete text-based interface for configuring all settings. See “Using the command line interface” on page 38.

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 11: NAT/Route mode settings

Administrator Password:		
Internal	IP: Netmask:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____
WAN1	IP: Netmask:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____
WAN2	IP: Netmask:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____
DMZ	IP: Netmask:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____
DMZ1 (FortiGate-100A	IP: Netmask:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____
DMZ2 (FortiGate-100A)	IP: Netmask:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____
ADSL (FortiGate-60ADSL)	IP: Netmask:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____
WLAN	IP: Netmask:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____
Network settings	Default Gateway:	_____ . _____ . _____ . _____
	(Interface connected to external network)	
	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 Internet Service Provider (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 12 to record the information you require for your PPPoE configuration.

Table 12: PPPoE setting

User name:	
Password:	

Using the web-based manager

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

For information about connecting to the web-based manager, see "Connecting to the web-based manager" on page 19.

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 > Options**.

2 Enter the IP address of the primary DNS server.

3 Enter the IP address of the secondary DNS server.

4 Select Apply.

Adding 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.

To add a default route

1 Go to **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.

Verifying the web-based manager configuration

To verify access settings, go to the interface you want to verify and select the edit icon. The Administrative Access field should have check marks beside the settings you chose in the preceeding steps.

Verify the connection

To verify your connection, try the following:

- browse to www.fortinet.com
- retrieve or send email from your email account

If you cannot browse to the web site or retrieve/send email from your account, review the previous steps to ensure all information was entered correctly and try again.

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 CLI” on page 22.

Configuring the FortiGate unit to operate in NAT/Route mode

Use the information you gathered in Table 11 on page 36 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 into the CLI.

2 Set the IP address and netmask of the internal interface to the internal IP address and netmask you recorded in Table 11 on page 36. 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 (WAN1) interface to the external IP address and netmask you recorded in Table 11 on page 36.

```
config system interface
   edit WAN1
      set mode static
      set ip <address_ip> <netmask>
 end
```

Example

```
config system interface
   edit WAN1
      set mode static
      set ip 204.23.1.5 255.255.255.0
 end
```

To set the WAN1 interface to use DHCP, enter:

```
config system interface
   edit WAN1
      set mode dhcp
 end
```

To set the WAN1 interface to use PPPoE, enter:

```
config system interface
    edit WAN1
        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
```

Adding 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.

To add a default route

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

```
config router static
    edit <seq_num>
        set dst <class_ip&net_netmask>
        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 WAN1:

```
config router static
  edit 1
  set dst 0.0.0.0 0.0.0.0
  set gateway 204.23.1.2
  set device wan1
  end
```

Verify the connection

To verify the connection, try the following:

- ping the FortiGate unit
- browse to the web-based manager GUI
- retrieve or send email from your email account

If you cannot browse to the web site or retrieve/send email from your account, review the previous steps to ensure all information was entered correctly and try again.

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

Connecting the FortiGate unit to the network(s)

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

The following network connections are available on the FortiGate unit:

- Internal for connecting to your internal network
- WAN1 for connecting to the Internet
- WLAN is the interface to the wireless LAN on the FortiWiFi models
- DMZ is the interface to the DMZ network

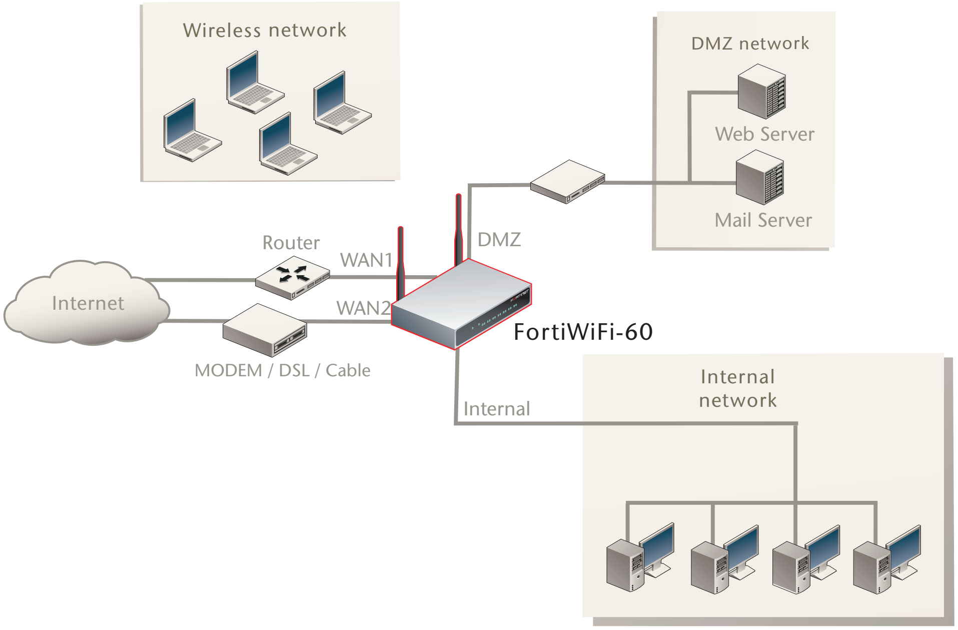
To connect the FortiGate unit

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. If you are a DSL or cable subscriber, connect the WAN1 interface to the internal or LAN connection of your DSL or cable modem.
3. Optionally connect the DMZ interface to your 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 your internal network.

Figure 10: FortiWiFi-60 NAT/Route mode connections



Configuring the networks

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

- For the internal network, 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 DMZ network, change the default gateway address of all computers and routers connected directly to your DMZ network to the IP address of the FortiGate DMZ interface.
- For the WAN network, change the default gateway address of all computers and routers connected to your WAN network to the IP address of the FortiGate WAN interface.
- For the WLAN network on the FortiWiFi-60/60M units, configure an IP address for the wireless local area network 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 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.

Transparent mode installation

This section describes how to install the FortiGate unit in Transparent mode. This section includes the following topics:

- Preparing to configure Transparent mode
- Using the web-based manager
- Using the Command line interface
- Connecting the FortiGate unit to your network.

Note: The ADSL interface will only function when using the FortiGate-60ADSL unit in NAT/Route mode. Changing to Transparent mode will disable the ADSL interface.

Preparing to configure Transparent mode

Use Table 13 on page 43 to gather the information you need to customize Transparent mode settings.

You can configure Transparent mode using one of the following methods:

- the web-based manager GUI
- the command line interface (CLI)

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 13: 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 19.

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 Type the Management IP/Netmask address and Default Gateway address you gathered in Table 13 on page 43.

5 Select Apply.

You do not have to reconnect to the web-based manager at this time. Once you select Apply, the changes are immediate, and you can go to the system dashboard to verify the FortiGate unit has changed to Transparent mode.

To configure DNS server settings

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

2 Enter the IP address of the primary DNS server.

3 Enter the IP address of the secondary DNS server.

4 Select Apply.

Using the Command line interface

As an alternative to the web-based manager, 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 CLI" on page 22. Use the information you gathered in Table 13 on page 43 to complete the following procedures.

To change to Transparent mode using the CLI

1 Make sure you are logged into the CLI.

2 Switch to Transparent mode. Enter:

```
config system settings
     set opmode transparent
     set manageip <address_ip> <netmask>
     set gateway <address_gateway>
  end
```

After a few seconds, the following prompt appears:

```
Changing to TP mode
```

3 When the login prompt appears, enter the following:

```
get system settings
```

The CLI displays the status of the FortiGate unit including the management IP address and netmask:

```
opmode          : transparent
manageip        : <address_ip><netmask>
```

You should verify the DNS server settings are correct. The DNS settings carry over from NAT/Route mode and may not be correct for your specific Transparent mode configuration. Use Table 13 on page 43 to configure the DNS server settings.

To verify the DNS server settings

Enter the following commands to verify the FortiGate unit's DNS server settings:

```
show system dns
```

The above CLI command should give you the following DNS server setting information:

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

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
```

Reconnecting to the web-based manager

When the FortiGate unit has switched to Transparent mode, you can reconnect to the web-based manager using the new IP address. Browse to https:// followed by the new IP address. If you connect to the management interface through a router, make sure you have added a default gateway for that route to the management IP default gateway field.

Connecting the FortiGate unit to your network

When you complete the initial configuration, you can connect the FortiGate unit between your internal network and the Internet and connect an additional network to the DMZ interface.

The modem connection is not available when using the FortiGate uni in transparent mode for the FortiGate-60M and FortiGate-60ADSL.

To connect the FortiGate unit running in Transparent mode:

1. Connect the Internal interface to the hub or switch connected to your internal network.
2. Connect the WAN1 interface to network segment connected to the external firewall or router.
   Connect to the public switch or router provided by your Internet Service Provider.
3. Connect the DMZ interface to another network.

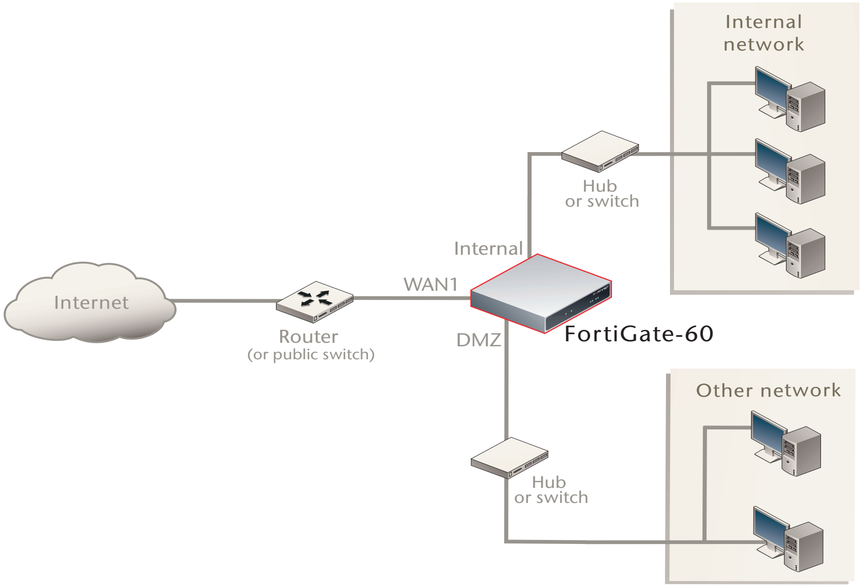
Verify the connection

To verify the connection, try the following:

- ping the FortiGate unit
- browse to the web-based manager GUI
- retrieve or send email from your email account

If you cannot browse to the web site or retrieve/send email from your account, review the previous steps to ensure all information was entered correctly and try again.

Figure 11: FortiGate-60 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.

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.

To set the date and time

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

7. Set the hour, minute, second, month, day, and year as required.
8. Select OK.

Note: If you choose the option Automatically adjust clock for daylight saving changes, the system time must be manually adjusted after daylight savings time ends.

To use NTP to set the FortiGate date and time

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

Register your FortiGate unit

After installing a new FortiGate unit, register the unit by visiting http://support.fortinet.com and select 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.

By registering your FortiGate unit, you will receive updates to threat detection and prevention databases (Antivirus, Intrusion Detection, etc.) and will also ensure your access to technical support.

Updating antivirus and IPS signatures

You can configure the FortiGate unit to connect to the FortiGuard Distribution Network (FDN) to update the antivirus (including grayware), antispam and IPS attack definitions.

The FDN is a world wide network of FortiGuard Distribution Servers (FDS). 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.

You can update your antivirus and IPS signatures using the web-based manager or the CLI. Before you can begin receiving updates, you must register your FortiGate unit from the Fortinet web page. For information about registering your FortiGate unit, see “Register your FortiGate unit” on page 47.

Note: Update AV and IPS signatures on a regular basis. If you do not update AV and IPS signatures regularly, the FortiGate unit can become vulnerable to new viruses.

After registering your FortiGate unit, verify the FortiGate unit can connect to the FDN:

- Check that the FortiGate unit’s system time is correct.
- From the web-based manager, select refresh from the FortiGuard Center.

If you cannot connect to the FDN, follow the procedure for registering your FortiGate unit and try again or see “Adding an override server” on page 49.

Updating antivirus and IPS signatures from the web-based manager

After you have registered your FortiGate unit, you can update antivirus and IPS signatures using the web-based manager. The FortiGuard Center enables you to receive push updates, allow push update to a specific IP address, and schedule updates for daily, weekly, or hourly intervals.

To update antivirus definitions and IPS signatures

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

2 Select Update Now to update the antivirus definitions.

If the connection to the FDN 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 FortiGuard Center page lists new version information for antivirus definitions. The System Status page also displays new dates and version numbers for the antivirus definitions. Messages are recorded to the event log indicating whether the update was successful or not.

Note: Updating antivirus definitions can cause a very short disruption in traffic currently being scanned while the FortiGate unit applies the new signature database. Schedule updates when traffic is light, for example overnight, to minimize any disruption.

Updating the IPS signatures from the CLI

You can update IPS signatures using the CLI. Use the following procedure to update IPS signatures.

Note: You can only update antivirus definitions from the web-based manager.

To update IPS signatures using the CLI

1 Log into the CLI.

2 Enter the following CLI command:

```
configure system autoupdate ips
  set accept-recommended-settings enable
  end
```

Scheduling antivirus and IPS updates

You can schedule regular, automatic updates of antivirus and IPS signatures, either from the web-based manager or the CLI.

To enable schedule updates from the web-based manager

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

2 Select the Scheduled Update check box.

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

Every	Once every 1 to 23 hours. Select the number of hours and minutes between each update request.
Daily	Once a day. You can specify the time of day to check for updates.
Weekly	Once a week. You can specify the day of the week and time of day to check for updates.

4 Select Apply.

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

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

To enable schedule updates from the CLI

1 Log into the CLI.

2 Enter the following command:

```
config system autoupdate schedule
     set day
     set frequency
     set status
     set time
  end
```

Example

```
config system autoupdate schedule
     set update every Sunday
     set frequency weekly
     set status enable
     set time 16:45
  end
```

Adding an override server

If you cannot connect to the FDN, or if your organization provides updates using their own FortiGuard server, use the following procedures to add the IP address of an override FortiGuard server in either the web-based manager or the CLI.

To add an override server from the web-based manager

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

2 Select the Use override server address check box.

3 Type the fully qualified domain name or IP address of a FortiGuard server.

4 Select Apply.

The FortiGate unit tests the connection to the override server.

If the FDN setting changes to available, the FortiGate unit has successfully connected to the override server.

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

To add an override server using the CLI

1 Log into the CLI.

2 Enter the following command:

```
config system autoupdate override
     set address
     set status
  end
```

Configuring the modem interface

The modem interface is available on the FortiGate-60 series only excluding the FortiGate-60ADSL.

The following section will cover how to configure the FortiGate-60M using the web-based manager. To configure the FortiGate-60 and FortiWiFi-60 modem, use the CLI.

The FortiGate-60 series includes support for a redundant or stand alone modem interface in NAT/Route mode.

- In redundant mode, the modem interface automatically takes over from a selected Ethernet interface when that Ethernet interface is unavailable.
- In stand alone mode, the modem interface is the connection from the FortiGate unit to the Internet.

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

This section includes the following topics:

Selecting a modem mode

The modem interface can work in one of two modes:

- redundant mode
- stand alone mode

Redundant mode configuration

The redundant modem interface serves as a backup to the Ethernet interface. If that Ethernet interface disconnects from its network, the modem automatically dials the configured dial-up account(s). When the modem connects to a dial-up account, the FortiGate unit routes IP packets normally destined for the selected Ethernet interface to the modem interface. During this time, the unit pings the Ethernet connection to check when it is back online.

When the Ethernet interface can connect to its network again, the FortiGate unit disconnects the modem interface and switches back to the Ethernet interface.

For the FortiGate unit 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.

To configure a redundant modem connection for the FortiGate-60M

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

2 Select Enable modem.

3 Select Redundant for the mode.

4 From the Redundant for list, select the Ethernet interface you want the modem to back up.

5 Configure other modem settings as required.

"Configuring modem settings" on page 53.

6 Configure a ping server for the Ethernet interface selected in step 4.

See "Adding a Ping Server" on page 58.

7 Configure firewall policies for connections to the modem interface.

See "Adding firewall policies for modem connections" on page 59.

To configure the FortiGate-60 and FortiWiFi-60 through the CLI

1 Log into the CLI.

2 Enter the following to configure a redundant modem:

```
config system modem
     set status enable
     set status mode redundant
   end
```

Stand alone mode configuration

In stand alone mode, you manually connect the modem to a dial-up 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 dial-up account.

If the connection to the dial-up account fails, the FortiGate unit modem automatically redials the number. The modem redials the ISP number based on the amount of times specified by the redial limit, or until it connects to a dial-up account.

In stand alone mode the modem interface replaces the external Ethernet interface. 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 stand alone mode for the FortiGate-60M

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

2 Configure other modem settings as required.

See “Configuring modem settings” on page 53.

Make sure there is correct information in one or more Dial-up Accounts.

3 Configure firewall policies for connections to the modem interface.

See “Adding firewall policies for modem connections” on page 59.

4 Select Dial Up.

The FortiGate unit initiates dialing into each dial-up account in turn until the modem connects to an ISP.

To operate in stand alone mode on the CLI

1 Log into the CLI.

2 Enter the following to configure a stand alone modem:

```
config system modem
    set status enable
    set status mode standalone
  end
```

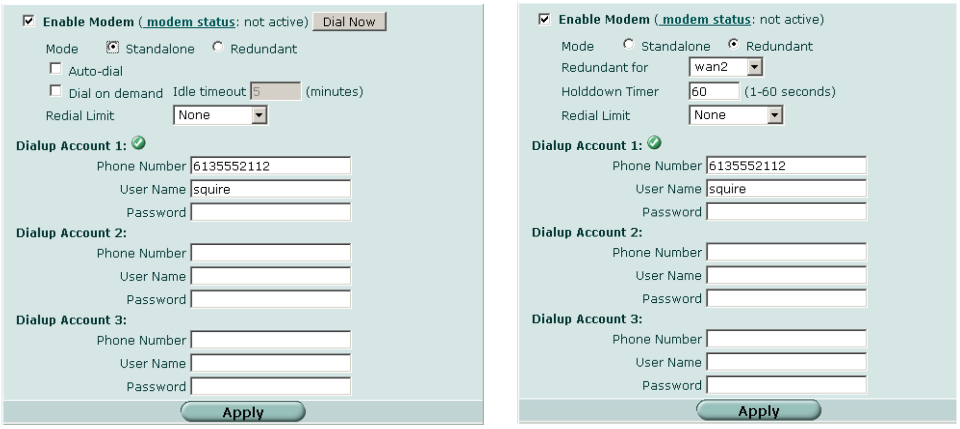
3 Enter the following to configure the dialup account:

```
config system modem
    set auto-dial
    set idle-timeout <minutes_interger>
    set passwd1 <passwrd_srt>
    set phone1 <phone-number_str>
    set redial <tries_interger>
    set username1 <name_str>
  end
```

Configuring modem settings

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

Figure 12: Modem settings (Stand alone and Redundant)



☑ Enable Modem (modem status: not active) Dial Now

Mode ● Standalone ○ Redundant

□ Auto-dial

□ Dial on demand Idle timeout 5 (minutes)

Redial Limit None

Dialup Account 1: ✓

Phone Number 6135552112

User Name squire

Password

Dialup Account 2:

Phone Number

User Name

Password

Dialup Account 3:

Phone Number

User Name

Password

Apply

☑ Enable Modem (modem status: not active)

Mode ○ Standalone ● Redundant

Redundant for wan2

Holddown Timer 60 (1-60 seconds)

Redial Limit None

Dialup Account 1: ✓

Phone Number 6135552112

User Name squire

Password

Dialup Account 2:

Phone Number

User Name

Password

Dialup Account 3:

Phone Number

User Name

Password

Apply

Enable Modem Select to enable the FortiGate modem.

Modem status The modem status shows one of the following: “not active”, “connecting”, “connected”, “disconnecting” or “hung up” (Stand alone mode only).

Dial Now/Hang Up (Stand alone mode only) Select Dial Now to manually connect to a dial-up account. If the modem is connected, you can select Hang Up to manually disconnect the modem.

Mode Select Stand alone or Redundant mode. In Stand alone mode, the modem is an independent interface. In Redundant mode, the modem is a backup facility for a selected Ethernet interface.

Auto-dial (Stand alone mode only) Select to dial the modem automatically if the connection is lost or the FortiGate unit is restarted. You cannot select Auto-dial if Dial on demand is selected.

Redundant for (Redundant mode only) Select the Ethernet interface the modem provides backup service.

Dial on demand (Stand alone mode only) Select to dial the modem when packets are routed to the modem interface. The modem disconnects after the idle timeout period. You cannot select Dial on demand if Auto-dial is selected.

Idle timeout (Stand alone mode only) Enter the timeout duration in minutes. After this period of inactivity, the modem disconnects.

Holddown Timer (Redundant mode only) Enter the time (1-60 seconds) the FortiGate unit waits before switching from the modem interface to the primary interface, after the primary interface has been restored. Configure a higher value if you find the FortiGate unit switching repeatedly between the primary interface and the modem interface.

Redial Limit The maximum number of times (1-10) the FortiGate unit modem attempts to reconnect to the ISP if the connection fails. Select None to have no limit on redial attempts.

Dialup Account Configure up to three dial-up accounts. The FortiGate unit tries connecting to each account in order until a connection can be established.

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.

You can configure and use the modem in NAT/Route mode only.

To configure modem settings

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

2 Select Enable Modem.

3 Change any of the dial-up connection settings.

4 Enter the settings for Dial-up Account 1 settings.

5 If you have multiple dial-up accounts, enter Phone Number, User Name, and Password for Dial-up Account 2 and Dial-up Account 3.

6 Select Apply.

Connecting and disconnecting the modem in Stand alone mode

To connect to a dial-up account

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

2 Select Enable Modem.

3 Make sure there is correct information in one or more Dial-up Accounts.

4 Select Apply if you make any configuration changes.

5 Select Dial Now.

The FortiGate unit initiates dialing into each dial-up account in turn until the modem connects to an ISP.

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 dial-up account.

The IP address and netmask are assigned to the modem interface. Go to **System > Network > Interface** to verify the IP address and netmask.

To disconnect the modem

Use the following procedure to disconnect the modem from a dial-up account.

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

2 Select Hang Up if you want to disconnect from the dial-up account.

Configuring the modem for the FortiGate-60 and FortiWiFi-60

Configure the modem settings for the FortiGate-60 and FortiWiFi-60 through the CLI. The following table of CLI commands are specifically for the FortiGate-60 and FortiWiFi-60 modem configuration.

Table 12: CLI commands for the FortiGate-60 and the FortiWiFi-60

Keywords and variables	Description	Default
`altmode {enable | disable}`	Enable for installations using PPP in China.	`enable`
`auto-dial {enable | disable}`	Enable to dial the modem automatically if the connection is lost, or the FortiGate unit is restarted. `dial-on-demand` must be disabled. `mode` must be `standalone`	disable
`connect_timeout <seconds>`	Set the connection completion timeout (30-255 seconds).	`90`
`dial-on-demand {enable | disable}`	Enable to dial the modem when packets are routed to the modem interface. The modem disconnects after the `idle-timer` period. `auto-dial` must be disabled. `mode` must be `standalone`.	disable
`holddown-timer <seconds>`	Used only when the modem is configured as a backup for an interface. Set 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. `mode` must be `redundant`.	`60`
`idle-timer <minutes>`	Set the number of minutes the modem connection can be idle before it is disconnected. `mode` must be `standalone`.	`5`
`interface <name>`	Enter an interface name to associate the modem interface with the Ethernet interface that you want to either back up (backup configuration) or replace (standalone configuration).	No default.
`mode <mode>`	Enter the required mode: • `standalone` The modem interface is the connection from the FortiGate unit to the Internet. • `redundant` The modem interface automatically takes over from a selected Ethernet interface when that Ethernet interface is unavailable.	`standalone`
`passwd1 <password_srt>`	Enter the password used to access the specified dialup account.	No default
`passwd2 <password_str>`	Enter the password used to access the specified dialup account.	No default.
`passwd3 <password_str>`	Enter the password used to access the specified dialup account	No default.

Table 12: CLI commands for the FortiGate-60 and FortiWiFi-60 continued

`peer_modem1 {actiontec | ascendTNT | generic}`	If the modem at phone1 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. This setting applies to models 50AM, 60M, and WiFi-60M only.	`generic`
`peer_modem2 {actiontec | ascendTNT | generic}`	If the modem at phone2 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. This setting applies to models 50AM, 60M, and WiFi-60M only.	`generic`
`peer_modem2 {actiontec | ascendTNT | generic}`	If the modem at phone3 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. This setting applies to models 50AM, 60M, and WiFi-60M only.	`generic`
`phone1 <phone-number>`	Enter 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	No default.
`phone2 <phone-number>`	Enter 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.	No default.
`phone3 <phone-number>`	Enter 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.	No default.
`redial <tries_interger>`	Set the maximum number of times (1-10) the FortiGate unit dials the ISP to restore an active connection on the modem interface. Select `none` to allow the modem to redial without a limit.	No default.
`status {disable | enable}`	Enable or disable modem support.	`disable`
`username1 <name_str>`	Enter the user name used to access the specified dialup account	No default.
`username2 <name_str>`	Enter the user name used to access the specified dialup account.	No default.
`username3 <name_str>`	Enter the user name used to access the specified dialup account.	No default.

Example

```
config system modem
    set action dial
    set status enable
    set holddown-time 5
    set interface wan1
    set passwd1 acct1passwd
    set phone1 1234567891
    set redial 10
    set username1 acct1user
  end
```

Adding a Ping Server

Adding a ping server is required for routing failover for the modem in redundant mode. A ping server confirms the connectivity to an Ethernet interface.

To add a ping server to an interface

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

Dead gateway detection

The FortiGate unit uses dead gateway detection to ping the Ping Server IP address to make sure the FortiGate unit can connect to this IP address.

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 above.

To modify the dead gateway detection settings

1. Go to **System > Network > 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 the gateway is no longer functioning.
4. Select Apply.

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 the *FortiGate Administration Guide*. 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 the *FortiGate Administration Guide*.

Configuring the ADSL interface

The ADSL modem interface is available on the FortiGate-60ADSL unit only.

This section describes how to configure the ADSL interface on a FortiGate-60ADSL unit. It only describes the differences between ADSL and other FortiGate interface configuration procedures. For more detailed information refer to the *FortiGate Administration Guide*.

The FortiGate-60ADSL unit contains an Asynchronous Digital Subscriber Line (ADSL) interface. This provides much higher communication speeds than standard telephone modems.

Note: The ADSL interface will only function when using the FortiGate unit in NAT/Route mode. Changing to Transparent mode will disable the ADSL interface.

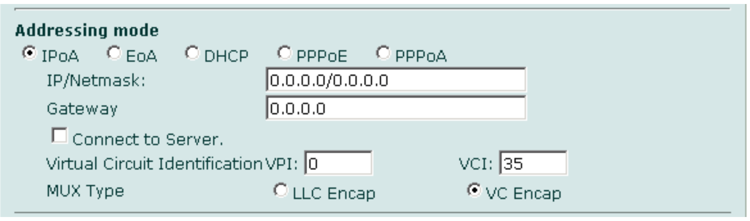
Configuring the ADSL interface using the web-based manager

The following procedures explain how to configure the ADSL interface to communicate with your ISP. Where indicated, you need to enter information that your ADSL ISP provides.

Configuring basic ADSL settings

The ADSL interface is configured like any other FortiGate physical network interface. The information that you need to provide depends on the addressing mode your ISP requires you to use. Static addressing using IPOA or EOA requires only an IP address and netmask. If you are using dynamic addressing, you need to configure it as described in "Configuring DHCP on the ADSL interface" on page 62 or "Configuring PPPoE or PPPoA on the ADSL interface" on page 63.

Go to **System > Network > Interface**. Select Create New or select the Edit icon of an existing interface. In the Addressing mode section, select IPoA or EoA.



Addressing mode

● IPoA ○ EoA ○ DHCP ○ PPPoE ○ PPPoA

IP/Netmask:	0.0.0.0/0.0.0.0		
Gateway	0.0.0.0		
□ Connect to Server.			
Virtual Circuit Identification VPI:	0	VCI:	35
MUX Type	○ LLC Encap	● VC Encap	

Address mode Select the addressing mode that your ISP specifies.

IPOA IP over ATM. Enter the IP address and netmask that your ISP provides.

EOA Ethernet over ATM, also known as Bridged mode. Enter the IP address and netmask that your ISP provides.

DHCP See "Configuring DHCP on the ADSL interface" on page 62.

PPPoE See "Configuring PPPoE or PPPoA on the ADSL interface" on page 63.

PPPoA See "Configuring PPPoE or PPPoA on the ADSL interface" on page 63.

Gateway Enter the default gateway.

Connect to Server Enable Connect to Server so that the interface automatically attempts to connect. Disable this option if you are configuring the interface offline.

Virtual Circuit Identification Enter the VPI and VCI values your ISP provides.

MUX Type Select the MUX type: LLC Encap or VC Encap.
Your ISP must provide this information.

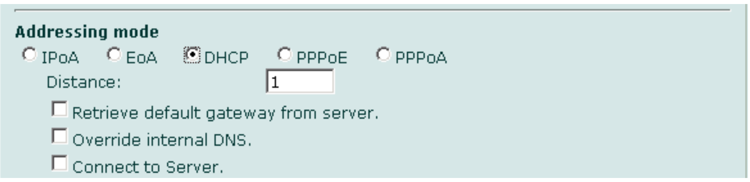
Configure other interface options as required. For more information see the *FortiGate Administration Guide*.

Configuring DHCP on the ADSL interface

If you configure an interface to use DHCP, the FortiGate unit automatically broadcasts a DHCP request. The interface is configured with the IP address and optionally DNS server addresses and default gateway address that the DHCP server provides.

Go to **System > Network > Interface**. Select Create New or select the Edit icon of an existing interface. In the Addressing mode section, select DHCP.

Figure 13: ADSL interface DHCP settings



Addressing mode
○ IPoA ○ EoA ● DHCP ○ PPPoE ○ PPPoA
Distance: 1
□ Retrieve default gateway from server.
□ Override internal DNS.
□ Connect to Server.

Distance Enter the administrative distance for the default gateway retrieved from the DHCP server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. The default distance for the default gateway is 1.

Retrieve default gateway from server Enable Retrieve default gateway from server to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table.

Override internal DNS Enable Override internal DNS to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page. You should also enable Obtain DNS server address automatically in **System > Network > Options**.

Connect to server Enable Connect to Server so that the interface automatically attempts to connect to a DHCP server. Disable this option if you are configuring the interface offline.

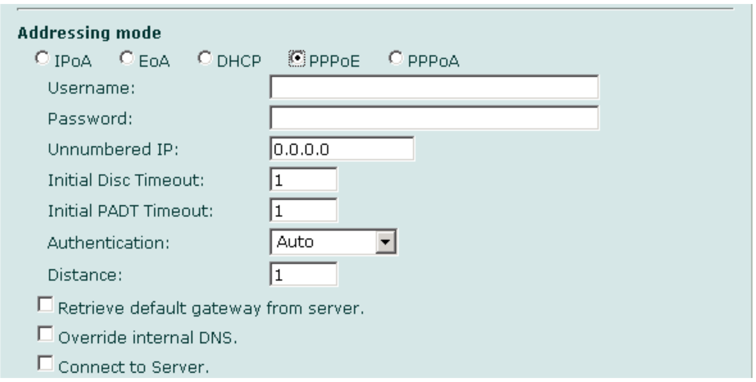
Configuring PPPoE or PPPoA on the ADSL interface

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

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

Go to **System > Network > Interface**. Select Create New or select the Edit icon of an existing interface. In the Addressing mode section, select PPPoE or PPPoA.

Figure 14: ADSL interface PPPoE or PPPoA settings



Addressing mode

○ IPoA ○ EoA ○ DHCP ● PPPoE ○ PPPoA

Username:

Password:

Unnumbered IP: 0.0.0.0

Initial Disc Timeout: 1

Initial PADT Timeout: 1

Authentication: Auto

Distance: 1

□ Retrieve default gateway from server.

□ Override internal DNS.

□ Connect to Server.

Enter the following information and select Apply.

Username Enter the PPPoE or PPPoA account user name that your ISP provides.

Password Enter the PPPoE or PPPoA account password that your ISP provides.

Unnumbered IP Specify the IP address for the interface. If your ISP has assigned you a block of IP addresses, use one of them. Otherwise, this IP address can be the same as the IP address of another interface or can be any IP address.

Initial Disc Timeout Initial discovery timeout. The time to wait before retrying to start a PPPoE discovery. Set Initial Disc to 0 to disable.

Initial PADT timeout Initial PPPoE or PPPoA Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE or PPPoA session if it is idle for this number of seconds. PADT must be supported by your ISP. Set initial PADT timeout to 0 to disable.

Authentication Select the authentication method your ISP uses: PAP, CHAP, MSCHAPv1, MSCHAPv2 or Auto.

Distance Enter the administrative distance for the default gateway retrieved from the PPPoE or PPPoA server. The administrative distance, an integer from 1-255, specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. The default distance for the default gateway is 1.

Retrieve default gateway from server Enable Retrieve default gateway from server to retrieve a default gateway IP address from a PPPoE or PPPoA server. The default gateway is added to the static routing table.

Override internal DNS Enable Override internal DNS to replace the DNS server IP addresses on the DNS page with the DNS addresses retrieved from the PPPoE or PPPoA server.

Connect to server Enable Connect to Server so that the interface automatically attempts to connect to a PPPoE or PPPoA server. Disable this option if you are configuring the interface offline.

Configuring the ADSL interface using the CLI

The ADSL interface is configured like any other FortiGate physical network interface. The information that you need to provide depends on the addressing mode your ISP requires you to use.

This section shows settings that are unique to the ADSL interface and are not described in other FortiGate documentation. Many settings that apply to interfaces generally also apply to the ADSL interface. This section shows only the settings that you might need to configure to communicate with your ISP. For a complete list of interface settings, refer to `system interface` in the *FortiGate CLI Reference*.

Command syntax

```
config system interface
  edit adsl
     set ip 10.10.10.1 255.255.255.0
     set mux_type vc-encaps
  ...
  end
```

Keywords and variables unique to the ADSL interface
These variables are available only in the `edit adsl` shell

Keywords and variables	Description	Default
`pppoe-mtu <mtu_bytes>`	Set custom maximum transmission unit (MTU) size in bytes for the ADSL interface PPPoE session. Ideally `mtu` should be the same as the smallest MTU of all the networks between this FortiGate unit and the destination of the packets. Range: 576 to 1492.	
`gwaddr <gw_ipv4>`	Gateway address. Available when `mode` is `ipoa or eoa`.	
`mux_type {llc-encap | vc-encaps}`	Enter the Mux mode of the virtual circuit.	
`vci`	Enter the virtual circuit identifier (VCI) your ISP provides.	35
`vpi`	Enter the virtual path identifier (VPI) your ISP provides.	0

General keywords and variables applicable to the ADSL interface
You might need to configure these settings to communicate with your ISP.

Keywords and variables	Description	Default
`auth-type <ppp_auth_method>`	Select the authentication method for PPPoE, PPPoA or DHCP: • Enter `auto` to select method automatically • Enter `chap` for CHAP • Enter `ms-chapv1` for Microsoft CHAP v1 • Enter `ms-chapv2` for Microsoft CHAP v2 • Enter `pap` for PAP `auth-type` is available only when `mode` is `pppoe`.	auto
`connection {enable | disable}`	Enable or disable connecting to a PPPoE or PPPoA server to configure the interface. This is available only when `mode` is `dhcp`, `pppoe` or `pppoa` and the unit is in NAT/Route mode.	`disable`
`defaultgw {enable | disable}`	Enable or disable the interface as the default gateway.	`disable`
`disc-retry-timeout <pppoe_retry_seconds>`	Set the initial discovery timeout in seconds. The time to wait before retrying to start a PPPoE discovery. Set `disc-retry-timeout` to 0 to disable. `mode` must be set to `pppoe`. This is available in NAT/Route mode only.	1
`dns-server-override {enable | disable}`	Enable to allow the interface to use DNS server addresses it acquired via DHCP or PPPoe. `mode` must be set to `dhcp` or `pppoe`.	`disable`
`edit <interface_name>`	Edit an existing interface or create a new VLAN interface.	None.
`gwdetect {enable | disable}`	Enable or disable confirming connectivity with the server at the `detectserver` IP address. The frequency with which the FortiGate unit confirms connectivity is set using the `failtime` and `interval` keywords in the command the `system global` command. For more information, see the *FortiGate CLI Reference*. This is available in NAT/Route mode only.	`disable`
`idle-timeout <pppoe_timeout_seconds>`	Disconnect if the PPPoE or PPPoA connection is idle for the specified number of seconds. This is available when `mode` is set to `pppoe` or `pppoa`.	0

General keywords and variables applicable to the ADSL interface
You might need to configure these settings to communicate with your ISP.

Keywords and variables	Description	Default
`ip <interface_ipv4mask>`	Enter the interface IP address and netmask. This is not available if `mode` is set to `dhcp, pppoa` or `pppoe`. This is available in NAT/Route mode only. The IP address cannot be on the same subnet as any other interface.	No default.
`ipunnumbered <unnumbered_ipv4>`	Enable IP unnumbered mode for PPPoE or PPPoA. Specify the IP address to be borrowed by the interface. This IP address can be the same as the IP address of another interface or can be any IP address. The Unnumbered IP may be used for PPPoE or PPPoA interfaces for which no unique local address is provided. If you have been assigned a block of IP addresses by your ISP for example, you can add any of these IP addresses to the Unnumbered IP.	No default.

`mode <interface_mode>`	Configure the connection mode for the interface. This is available only in NAT/Route mode.
	`dhcp`
	• Configure the interface to receive its IP address from a DHCP server.
	`pppoe`
	• Configure the interface to receive its IP address from a PPPoE server.
	`pppoa`
	• Configure the interface to receive its IP address from a PPPoA server.
	`eoa`
	• Configure a static IP address for the interface in ADSL EoA bridge mode.
	`ipoa`
	• Configure a static IP address for the interface in ADSL IPoA route mode.
		`eoa`

`mtu <mtu_bytes>`	Set custom maximum transmission unit (MTU) size in bytes. Ideally `mtu` should be the same as the smallest MTU of all the networks between this FortiGate unit and the destination of the packets. For `static` mode the `<mtu_bytes>` range is 576 to 1500 bytes. For `dhcp` mode the `<mtu_bytes>` range is 576 to 1500 bytes. For `pppoe` mode the `<mtu_bytes>` range is 576 to 1492 bytes. In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces to match the new MTU. This is available when `mtu-override` is enabled.	1500
`mtu-override {enable | disable}`	Select enable to use custom MTU size instead of default (1500).	`disable`

General keywords and variables applicable to the ADSL interface You might need to configure these settings to communicate with your ISP.		
Keywords and variables	**Description**	**Default**
`padt-retry-timeout <padt_retry_seconds>`	Initial PPPoE Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP. Set PADT timeout to 0 to use default. This is available when `mode` is `ppoe`. This is available in NAT/Route mode only.	1
`password <pppoe_password>`	Enter the password to connect to the PPPoE or PPPoA server. This is available when `mode` is `ppoe` or `pppoa`. This is available in NAT/Route mode only.	No default.
`status {down | up}`	Start or stop the interface. If the interface is stopped it does not accept or send packets. If you stop a physical interface, VLAN interfaces associated with it also stop.	`up` (`down` for VLANs)
`username <pppoe_username>`	Enter the user name to connect to the PPPoE or PPPoA server. This is available in NAT/Route mode when `mode` is set to `pppoe` or `pppoa`.	No default.

Example - IPOA or EOA

This example shows the settings required to use an IP address of 10.10.10.1 and a netmask of 255.255.255.0 with IPOA using PPPoE and custom VPI and VCI settings. This example also applies to the EOA mode if you change the `mode` setting to `eoa`.

```
config system interface
  edit adsl
     set mode ipoa
     set ip 10.10.10.1 255.255.255.0
     set vpi 1
     set vci 34
     set mux-type llc-encaps
     set connection enable
  end
end
```

Example - DHCP

This example shows the settings required to connect to an ISP using DHCP with default VCI and VPI settings.

```
config system interface
  edit adsl
     set mode dhcp
     set mux-type llc-encaps
     set connection enable
  end
end
```

Example - PPPoE or PPPoA

This example shows the settings required to connect to an ISP using default VCI and VPI settings. This example also applies to the PPPoA mode if you change the `mode` keyword to `pppoa`.

```
config system interface
  edit adsl
     set mode pppoe
     set username user1
     set password hard_to_guess
     set auth-type pap
     set mux-type llc-encaps
     set connection enable
  end
end
```

Adding firewall policies for ADSL connections

The ADSL interface requires firewall addresses and policies. You can add one or more addresses to the ADSL interface. For information about adding addresses, see the *FortiGate Administration Guide*. When you add addresses, the ADSL interface appears on the policy grid.

You can configure firewall policies to control the flow of packets between the ADSL interface and the other interfaces on the FortiGate unit. For information about adding firewall policies, see the *FortiGate Administration Guide*.

Using a wireless network

This chapter is specifically for the FortiWiFi-60 units.

In a wired network, computers are connected through a series of cables that transfer information. In a wireless network, information is transferred over radio waves. There are factors which affect the transmission of data “on the air” that you must take into account when setting up a wireless network.

This section outlines the considerations for wireless networking and steps you can take to make your wireless network as efficient as possible.

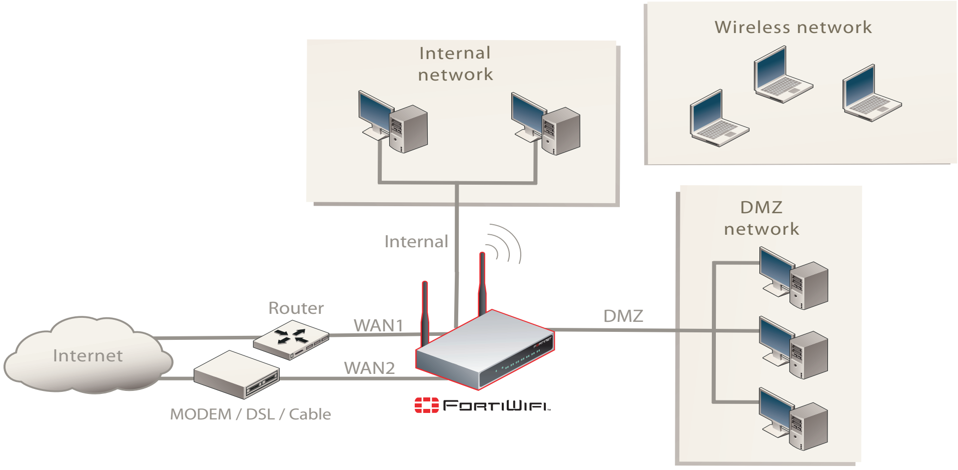
This section includes the following topics:

- Setting up a wireless network
- Wireless Security
- FortiWiFi-60 operation modes
- Setting up the FortiWiFi-60 as an Access Point

Setting up a wireless network

In its simplest form, a wireless network is an Access Point communicating with one wireless device. An Access Point (AP) is a device that provides a communications hub for a wireless network. The AP and the wireless devices operate on a common radio channel. The FortiWiFi-60 acts as an AP and assigns all wireless users to the same subnet. With the proper firewall policies and routing, wireless users can communicate with users on the internal network or on an external network such as the Internet.

Figure 15: FortiWiFi-60 as an Access Point



Positioning an Access Point

When placing the FortiWiFi-60 AP, your main concern is providing a strong signal to all users. A strong signal ensures a fast connection and the efficient transfer of data. A weaker signal means a greater chance of data transmission errors and the need to re-send information, slowing down data transfer.

Consider the following guidelines when placing the FortiWiFi-60 AP:

- Physical barriers can impede the radio signals. Solid objects such as walls, furniture and people absorb radio waves, weakening the signal. Be aware of the physical barriers in your office space that may reduce a signal. If there is enough physical interference, you may encounter dead spots that receive no signals.
- Ensure the FortiWiFi-60 AP is located in a prominent location within a room for maximum coverage, rather than in a corner.
- Construction materials used in a building can also weaken radio signals. Rooms with walls of concrete or metal can affect the signal strength.

Radio Frequency interface

The 802.11 standard uses a frequency range of 2.4 to 2.483 GHz. Radio frequency (RF) interference occurs when other devices send RF signals during their normal operation that use the same frequency as the FortiWiFi-60 AP. Wireless devices such as 2.4 GHz cordless phones, microwave ovens and Bluetooth devices can interfere with packet transmissions on a wireless network.

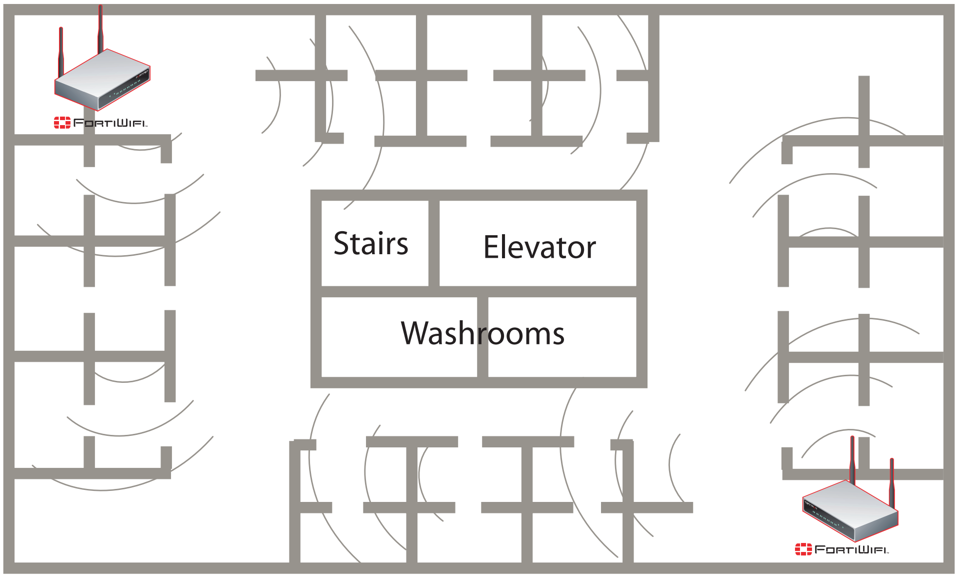
To avoid RF interference:

- Remove these devices from the immediate area where users are working. Something as simple as a Bluetooth enabled mouse may cause transmission interruptions.
- Keep the FortiWiFi-60 AP and wireless devices at least 10 feet away from appliances such as microwave ovens and cordless phones.
- If you must have a cordless phone, select one that does not use the 2.4GHz frequency range.
- Consider more FortiWiFi-60 APs to help strengthen the signal. The weaker the signal, the slower the transmission will be as it tries to compete against other wireless devices.
- Set a channel that users and FortiWiFi-60 APs will specifically use can improve signal quality.

Using multiple access points

If you cannot avoid some of these impediments due to the shape of the office or building materials used, you may need to use multiple FortiWiFi-60 APs to help distribute the radio signal around the room. Figure 16 shows how positioning two FortiWiFi-60 APs within a uniquely shaped office space helps to distribute signals around the area.

Figure 16: Using multiple APs to provide a constant strong signal.



This sample office has washrooms, a stairwell and an elevator shaft in the center of the building, making it impossible to use a single FortiWiFi-60 AP effectively. The elevator shaft and multiple metal stalls in the washrooms can cause signal degradation. However, placing a FortiWiFi-60 AP in opposite corners of the office provides maximum coverage.

When using multiple APs, each FortiWiFi-60 AP should be set to a different channel to avoid interference in areas where signals from both FortiWiFi-60 devices can be received.

Wireless Security

Radio waves transmitted between a wireless device and access points provide the weakest link between the wireless device and network servers. Wireless networking can be risky because information travels on radio waves, which is a public medium. The 802.11 standard includes security options to stop your information from being intercepted by unwanted sources. These are Wireless Equivalent Privacy (WEP) and WiFi Protected Access (WPA) encryption. Wireless encryption is only used between the wireless device and the AP. The AP decrypts the data before sending it along the wired network. The FortiWiFi-60 supports both encryption methods.

Wireless Equivalent Privacy (WEP)

WEP security uses an encryption key between the wireless device and the AP. For WEP security, the wireless device and AP must use the same encryption key, and is manually typed by the wireless user and administrator. When activated, the wireless device encrypts the data with the encryption key for each frame using RSA RC4 ciphers.

There has been criticism of WEP security. WEP keys are static. They must be changed manually and frequently on both the wireless device and the APs. On a small company or network with a few users and APs, this is not a big issue. However, the more users and APs, changing WEP keys regularly can become an administrative headache and potentially error prone. Consequently, keys are rarely changed over months or years, leaving a hacker plenty of time to get the key and gain access to the network.

In small wireless networking environments, activating WEP security will significantly minimize outside infiltrators from getting in your network and is better than no security at all. However, it is still very important that you regularly change the WEP key, at least weekly; or monthly at most.

Wi-Fi Protected Access (WPA)

WPA was developed to replace the WEP standard and provide a higher level of data protection for wireless networks. WPA provides two methods of authentication; through 802.1X authentication or pre-shared keys.

802.1X authenticates users through an EAP authentication server such as a RADIUS server authenticates each user before they can connect to the network. The encryption keys can be changed at varying intervals to minimize the opportunity for hackers to crack the key being used.

In a network setup where a RADIUS server is not a viable option, WPA also provides authentication with preshared keys using Temporal Key Integrity Protocol (TKIP). Using TKIP, the encryption key is continuously re-keyed while the user is connected to the wireless network. This creates a unique key on every data packet. To further ensure data integrity, a Message Integrity Code (MIC also known as Michael) is incorporated into each packet. It uses an 8 byte message integrity code that is encrypted using the MAC addresses and data from each frame to provide a more secure packet transmission.

WPA provides a more robust security between the wireless device and the access point. The FortiWiFi-60/60M device supports both WPA methods.

Additional security measures

The FortiWiFi-60 includes other security measures you can use to block unwanted users from accessing your wireless network. By setting a few extra options, you can be assured your network and its information is secure.

MAC address filtering

To improve the security of your wireless network, consider enabling MAC address filtering on the FortiWiFi-60 unit. By enabling this feature, you define the wireless devices that can access the network based on their system MAC address. When a user attempts to access the wireless network, the FortiWiFi-60 unit checks the MAC address of the user to the list you created. If the MAC address is on the approved list, the user gains access to the network. If the user is not in the list, the user is rejected. Using MAC address filtering makes it more difficult for a hacker using random MAC addresses or spoofing a MAC address to gain access to your network.

Service Set Identifier

The Service Set Identifier (SSID) is the network name shared by all users on a wireless network. Wireless users should configure their computers to connect to the network that broadcasts this network name. For security reasons, do not leave the default name of “fortinet” as the network name.

Broadcasting enables wireless users to find a network. The FortiWiFi-60 models includes an option not to broadcast the SSID. This provides an extra layer of protection. If you configure all wireless users to the correct SSID, you do not need to enable the broadcasting of the SSID.

To disable SSID

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

2 Select Disable for the SSID Broadcast.

3 Select OK.

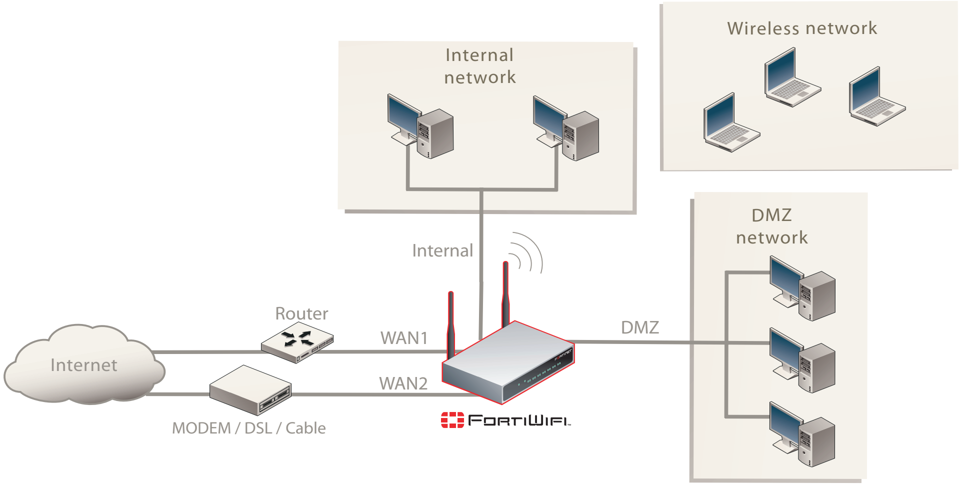
FortiWiFi-60 operation modes

The FortiWiFi-60 models each have two modes of operation for wireless networking: Access Point and Client.

Access Point mode

When using the Forti-WiFi-60 in Access Point mode, the device acts as an access point for wireless users to connect to, send and receive information over a wireless network. It enables multiple wireless network users access to the network without the need to connect to it physically. The FortiWiFi-60 can connect to the internal network and act as a firewall to the Internet. Access Point mode is the default mode.

Figure 17: FortiWiFi60 in Access Point mode

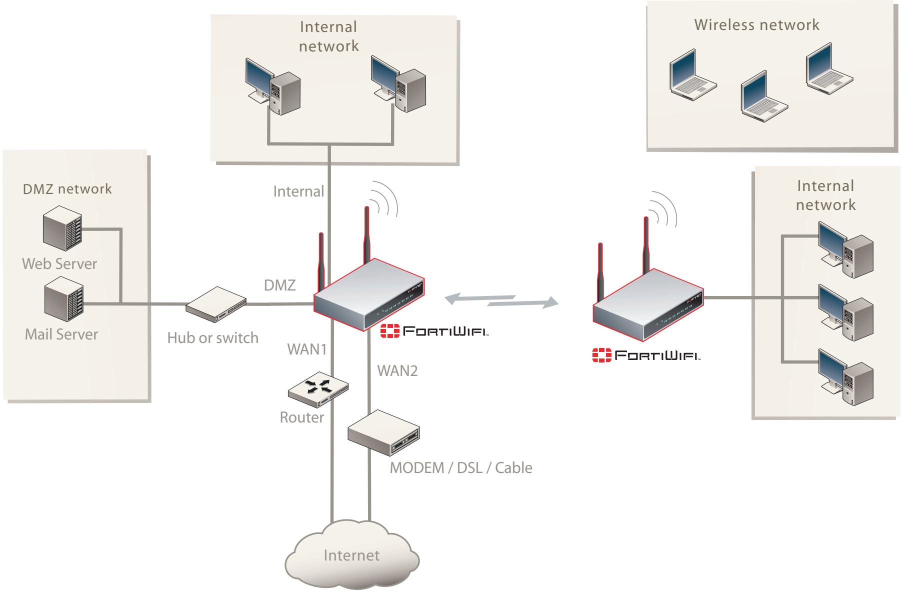


Client mode

When using the FortiWiFi-60 in Client mode, the device is set to receive transmissions from another access point. This enables you to connect remote users to an existing network using wireless protocols from a location that does not have a wired infrastructure.

For example, in a warehouse where shipping and receiving are on opposite sides of the building, running cables is not an option due to the warehouse environment. The FortiWiFi-60 unit can support wired users using its four Ethernet ports and can connect to another Access Point wirelessly as a Client. This connects the wired users to the network using the 802.11 wireless standard as a backbone.

Figure 18: FortiWiFi-60/60M in Client mode



Changing the operating mode

To change the wireless operating mode

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

2 For the Operation mode, select Change

3 Select the desired operation mode and select OK.

Setting up the FortiWiFi-60 as an Access Point

This section describes how to quickly configure the FortiWiFi-60 unit as an AP to allow network access for wireless workstations located on the same wireless LAN as the unit. It also describes how to configure firewall policies and wireless security features to provide a secure wireless environment. For initial setup, use a desktop computer on the internal network with TCP/IP set as a DHCP client

This section contains the following steps:

- Set the DHCP settings
- Set the security options
- Configure the firewall policies

Set the DHCP settings

Configure a DHCP server for the FortiWiFi-60 WLAN interface. As a DHCP server, the interface dynamically assigns IP addresses to hosts on the network connected to the WLAN interface.

To configure the FortiWiFi-60/60M to be a DHCP server

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

2 Select the blue triangle to expand the WLAN options.

3 Configure the DHCP server settings:

Name: Enter a name of the DHCP sever. For example, DHCPSever_1.

Enable: Select to enable the DHCP Server.

Type: Select regular unless you are configuring for remote clients who will have an IPSec VPN connection to the WLAN interface.

IP Range: Enter the IP address of the WLAN to configure the IP address range. For example, 10.10.80.1 to 10.10.80.20.

Network Mask: Enter the network mask you created in Table 9 on page 35.

Domain: Enter domain name, for example, www.fortinet.com.

Lease Time: The expiry date of an IP address. This feature specifies either an unlimited or limited timeframe of an IP address.

Advanced: Use only to specify several DNS servers (including WIN servers) for the interface.

4 Select OK.

Note: The IP range must match the subnet address of the network where the DHCP request was received. Usually this would be the subnet connected to the WLAN interface.

Set the security options

To ensure proper security and protection of your network and its information, set the security options for the FortiWiFi-60 unit.

To set the data security

1. Go to **System > Wireless > Settings**.
2. Enter an SSID.
3. Set the SSID Broadcast to either enable or disable.
4. Select a Security mode.
5. Enter a key or pre-shared key depending on the Security Mode selected.
6. Select the MAC Filter tab.
7. Enable MAC filtering if desired.
8. Enter the MAC addresses and select to Allow or Deny them from the wireless network.

Note: You will need to distribute the information entered in step 2 and step 5 with the wireless users so they can connect to the wireless network.

Note: It is highly recommended you do not select “None”. Selecting None will leave your wireless network prone to hackers.

Configure the firewall policies

The FortiWiFi-60 provides WAN interfaces for Internet connections. You can configure the Internet connection for both wired networks on the internal and/or DMZ interfaces and the wireless network through the WLAN interface.

You can provide secure Internet access for wireless clients by creating firewall policies from the WLAN interface to the WAN1 or WAN2 interfaces.

The following example creates a policy from the wireless clients (WLAN interface) to the Internet (WAN1 interface) using traffic shaping, firewall authentication and the default Strict content policy.

To create a new wall policy for a secure Internet connection

1. Go to **Firewall > Policy**.
2. Select the blue arrow for WLAN to WAN1.
3. Select Create New.

Configure the following settings:

Interface/Zone Source	WLAN
Interface/Zone Destination	WAN1
Address Name Source	All
Address Name Destination	All
Schedule	Always
Service	ANY
Action	ACCEPT

NAT	Enable
Protection Profile	Strict

4 Select Advanced.

5 Select Traffic Shaping.

6 Configure traffic shaping bandwidth and Traffic Priority settings to meet your requirements.

7 Select OK.

FortiGate Firmware

Fortinet periodically updates the FortiGate firmware to include enhancements and address issues. After you have registered your FortiGate unit, FortiGate firmware is available for download at http://support.fortinet.com.

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

This section includes the following topics:

- Upgrading to a new firmware version
- Reverting to a previous firmware version
- Installing firmware images from a system reboot using the CLI
- The FortiUSB key
- Testing a new firmware image before installing it
- Installing and using a backup firmware image (FortiGate-100A only)

Note: If you have an earlier version of the FortiOS firmware, for example FortiOS v2.50, upgrade to FortiOS v2.80MR11 before upgrading to FortiOS v3.0.

Upgrading to a new firmware version

Use the web-based manager or CLI procedure to upgrade to a new FortiOS firmware version or to a more recent build of the same firmware version.

Upgrading the firmware using the web-based manager

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

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

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

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. Under **System Information > Firmware Version**, select Update.

5 Type the path and filename of the firmware image file, or select Browse and locate the file.

6 Select OK.

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

7 Log into the web-based manager.

8 Go to **System > Status** and check the firmware version to confirm the firmware upgrade is successfully installed.

9 Update antivirus and attack definitions. For information about updating antivirus and attack definitions, see the *FortiGate Administration Guide*.

Upgrading the firmware using the CLI

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

Note: Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. You can also use the CLI command `execute update-now` to update the antivirus and attack definitions. For details, see the *FortiGate Administration Guide*.

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

To upgrade the firmware using the CLI

1 Make sure the TFTP server is running.

2 Copy the new firmware image file to the root directory of the TFTP server.

3 Log into the CLI.

4 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 TFTP <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

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

The FortiGate unit responds with the message:

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

6 Type `y`.

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

7 Reconnect to the CLI.

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

```
get system status
```

9 Update antivirus and attack definitions (see the *FortiGate Administration Guide*), or from the CLI, enter:

```
execute update-now
```

Reverting to a previous firmware version

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

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.

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

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

Before beginning this procedure, it is recommended that you:

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

For more information, see the *FortiGate Administration Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v3.0 to FortiOS v2.80), 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, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. For details, see the *FortiGate Administration Guide*. You can also use the CLI command `execute update-now` to update the antivirus and attack definitions.

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

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

1 Copy the firmware image file to the management computer.

2 Log into the FortiGate web-based manager.

3 Go to **System > Status**.

4 Under **System Information > Firmware Version**, select Update.

5 Type the path and filename of the firmware image file, or select Browse and locate the file.

6 Select OK.

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

7 Log into the web-based manager.

8 Go to **System > Status** and check the Firmware Version to confirm the firmware is successfully installed.

9 Restore your configuration.

For information about restoring your configuration, see the *FortiGate Administration Guide*.

10 Update antivirus and attack definitions.

For information about antivirus and attack definitions, see the *FortiGate Administration Guide*.

Reverting to a previous firmware version using the CLI

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

Before beginning this procedure, it is recommended that you:

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

For more information, see the *FortiGate Administration Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v3.0 to FortiOS v2.80), 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, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. For details, see the *FortiGate Administration Guide*. You can also use the CLI command `execute update_now` to update the antivirus and attack definitions.

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

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

To revert to a previous firmware version using the CLI

1 Make sure the TFTP server is running.

2 Copy the firmware image file to the root directory of the TFTP server.

3 Log into the FortiGate CLI.

4 Make sure the FortiGate unit can connect to the TFTP server.

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

```
execute ping 192.168.1.168
```

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

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

Where `<name_str>` is the name of the firmware image file and `<tftp_ip4>` is the IP address of the TFTP server. For example, if the firmware image file name is `v28image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image TFTP v28image.out

192.168.1.168
```

The FortiGate unit responds with the message:

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

6 Type `y`.

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

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

7 Type `y`.

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

8 Reconnect to the CLI.

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

```
get system status
```

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

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

11 Update antivirus and attack definitions.

For information, see the *FortiGate Administration Guide*, or from the CLI, enter:

```
execute update-now
```

Installing firmware images from a system reboot using the CLI

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

Use this procedure to install a new firmware version or revert to a previous firmware version. To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9 serial cable. This procedure reverts the FortiGate unit to its factory default configuration.

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

For this procedure you:

- Access the CLI by connecting to the FortiGate console port using a RJ-45 to DB-9 serial cable.
- Install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, it is recommended that you:

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

  For more information, see the *FortiGate Administration Guide*.

If you are reverting to a previous FortiOS version (for example, reverting from FortiOS v3.0 to FortiOS v2.80), 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, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date. For information, see the *FortiGate Administration Guide*.

To install firmware from a system reboot

1. Connect to the CLI using the RJ-45 to DB-9 cable/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 the internal interface is connected to the same network as the TFTP server.
5. To confirm the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168, enter:

```
execute ping 192.168.1.168
```

6 Enter the following command to restart the FortiGate unit:

```
execute reboot
```

The FortiGate unit responds with the following message:

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

7 Type y.

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

When one of the following messages appears:

- FortiGate unit running v2.x BIOS

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

- FortiGate unit running v3.x BIOS

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

Immediately press any key to interrupt the system startup.

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

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

- FortiGate unit running v2.x BIOS

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

  Go to step 9.

- FortiGate unit running v3.x BIOS

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

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

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

The following message appears:

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

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

The following message appears:

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

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

The IP address can be any IP address that is valid for the network the interface is connected to. Make sure you do not enter the IP address of another device on this network.

The following message appears:

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

11 Enter the firmware image filename and press Enter.

The TFTP server uploads the firmware image file to the FortiGate unit and messages similar to the following are displayed:

- FortiGate unit running v2.x BIOS

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

  Type `y`.

- FortiGate unit running v3.x BIOS

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

  or

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

12 Type `D`.

The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

Restoring the previous configuration

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

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

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

For more information, see the *FortiGate Administration Guide*

If you are reverting to a previous firmware version (for example, reverting from FortiOS v3.0 to FortiOS v2.80), you might not be able to restore your previous configuration from the backup up configuration file.

The FortiUSB key

The FortiUSB key provides flexibility and control when backing up and restoring configuration files. The FortiUSB key also enables you to have a single, secure location for storing configuration files.

The FortiUSB key is used with the USB Auto-Install feature, automatically installing a configuration file and a firmware image file on a system reboot. The USB Auto-Install feature uses a configuration file and a firmware image file that is on the FortiUSB key, and on a system reboot, checks if these files need to be installed. If they do, the FortiGate unit installs the configuration file and firmware image file directly from the key to the unit.

Note: The FortiUSB key is purchased separately. The FortiGate unit only supports the FortiUSB key available from Fortinet.

Inserting and removing the FortiUSB key from the FortiGate unit

To ensure the FortiGate unit recognizes that they key is either inserted or removed from the device, you must use the following steps to properly insert the key. Properly removing the FortiUSB key ensures the files are protected from accidentally being lost or deleted.

Note: When the FortiUSB key is inserted, the FortiGate unit boots from the flash. If the USB Auto-Install feature is enabled, the unit checks if a different image or configuration file needs to be installed.

To properly insert the FortiUSB key

1. Use the CLI interface to shutdown the FortiGate unit.
2. Disconnect the power supply from the FortiGate unit once the following message appears:

```
The system is halted
```

3. Insert the FortiUSB key into the USB port on the FortiGate unit.
4. Connect the power supply to the FortiGate unit to restart the system.

The FortiUSB key is now inserted in the FortiGate unit.

To properly remove the FortiUSB key

1. Use the CLI interface to shutdown the FortiGate unit.
2. Disconnect the power supply from the FortiGate unit once the following message appears:

```
The system is halted
```

3. Remove the FortiUSB key from the USB port on the FortiGate unit.
4. Connect the power supply to the FortiGate unit to reboot the system.

Backup and Restore from the FortiUSB key

You can use the FortiUSB key to either backup a configuration file or restore a configuration file.

You should always make sure the FortiUSB key is properly install before proceeding since the FortiGate unit must recognize that the key is installed in its USB port. The FortiUSB key may not be recognized by the FortiGate unit if it is inserted when the unit is running. If the key is unrecognized by the FortiGate unit, you will be unable to properly backup your configuration. See "Inserting and removing the FortiUSB key from the FortiGate unit" on page 87 for more information about inserting the FortiUSB key.

Note: You can only save VPN certificates if you encrypt the file. Make sure the configuration encryption is enabled so you can save the VPN certificates with the configuration file. However, an encrypted file is ineffective if selected for the USB Auto-Install feature.

To backup configuration using the web-based manager

1. Go to **System > Maintenance > Backup and Restore**.
2. Select USB Disk from the backup configuration to list.
3. Enter a filename for the configuration file.
4. Select Backup.

To restore configuration web-based manager

1. Go to **System > Maintenance > Backup and Restore**.
2. Select USB Disk from the restore configuration from list.
3. Select a backup configuration file from the list.
4. Select Restore.

To backup configuration using the CLI

1. Log into the CLI.
2. Enter the following command to backup the configuration files:

   ```
   exec backup config usb <filename>
   ```
3. Enter the following command to check the configuration files are on the key:

   ```
   exec usb-disk list
   ```

To restore configuration using the CLI

1. Log into the CLI.
2. Enter the following command to restore the configuration files:

   ```
   exec restore image usb <filename>
   ```

   The FortiGate unit responds with the following message:

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

Using the USB Auto-Install feature

The USB Auto-Install feature automatically updates the FortiGate configuration file and image file on a system reboot. Also, this feature provides you with an additional backup if you are unable to save your system settings before shutting down or rebooting your FortiGate unit.

You need to do the following before configuring the USB Auto-Install feature:

- power off the FortiGate unit
- install the FortiUSB key
- power up the FortiGate unit

See "Inserting and removing the FortiUSB key from the FortiGate unit" on page 87 for more information on inserting the FortiUSB key.

The following procedures use both the web-based manager and the CLI. However, it is recommended you use the CLI since the login screen may appear before the installation is complete. The FortiGate unit may reboot twice if installing the firmware image and configuration file.

Note: You need an unencrypted configuration file for this feature. Also the default files, image.out and fgt_system.conf, must be in the root directory.

Note: Make sure FortiOS v3.0MR1 is installed on the FortiGate unit before installing.

To configure the USB Auto-Install using the web-based manager

1. Go to **System > Maintenance > Backup and Restore**.
2. Select the blue arrow to expand the Advanced options.
3. Select the following:
   - On system restart, automatically update FortiGate configuration file if default filename is available on the USB disk.
   - On system restart, automatically update FortiGate firmware image if default image is available on the USB disk.
4. Enter the configuration and image filenames or use the default configuration filename (system.conf) and default image name (image.out).
5. The default configuration filename should show in the Default configuration file name field.
6. Select Apply.

To configure the USB Auto-Install using the CLI

1. Log into the CLI.
2. Enter the following command:

```
config system auto-install
  set default-config-file <filename>
  set auto-intall-config <enable/disable>
  set default-image-file <filename>
  set auto-install-image <enable/disable>
end
```

3. Enter the following command to see the new firmware installation settings:

```
get system status
```

Additional CLI Commands for the FortiUSB key

Use the following CLI commands when you want to delete a file from the FortiUSB key, list what files are on the key, including formatting the key or renaming a file:

- `exec usb-disk list`
- `exec usb-disk delete <filename>`
- `exec usb-disk format`
- `exec usb-disk rename <old_filename1> <old_filename2>`

Note: If you are trying to delete a configuration file from the CLI command interface, and the filename contains spaces, you will need quotations around the filename before you can delete the file from the FortiUSB key.

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 79.

Use this procedure to test a new firmware image before installing it. To use this procedure, you must connect to the CLI using the RJ-45 to DB-9 serial cable/console port. This procedure temporarily installs a new firmware image using your current configuration.

For this procedure you:

- Access the CLI by connecting to the FortiGate console port using a RJ-45 to DB-9 serial cable/console port.
- 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 RJ-45 to DB-9 serial cable/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 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 unit starts, a series of system startup messages are displayed.

   When one of the following messages appears:

   - FortiGate unit running v2.x BIOS

     ```
     Press Any Key To Download Boot Image.
     ...
     ```
   - FortiGate unit running v3.x BIOS

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

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

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

   - FortiGate unit running v2.x BIOS

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

     Go to step 9.
   - FortiGate unit running v3.x BIOS

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

     Enter G,F,Q,or H:
     ```
8. Type G to get the new firmware image from the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```
9. Type the address of the TFTP server and press Enter.

   The following message appears:

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

10 Type an IP address that can be used by the FortiGate unit to connect to the TFTP server.

The IP address can be any IP address that is valid for the network the interface is connected to. Make sure you do not enter the IP address of another device on this network.

The following message appears:

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

11 Enter the firmware image file name and press Enter.

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

- FortiGate unit running v2.x BIOS

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

  Type `n`.
- FortiGate unit running v3.x BIOS

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

  or

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

12 Type `R`.

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

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

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

```
get system status
```

You can test the new firmware image as required.

Installing and using a backup firmware image

The following procedures are specific to the FortiGate-100A only.

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

Installing a backup firmware image

To run this procedure you:

- Access the CLI by connecting to the FortiGate console port using a RJ-45 to DB-9 serial cable/console port,

- Install a TFTP server that you can connect to from the FortiGate as described in the procedure "Installing firmware images from a system reboot using the CLI" on page 84.

To install a backup firmware image

1. Connect to the CLI using the RJ-45 to DB-9 serial cable/console port.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of your TFTP server.
4. To confirm the FortiGate unit can connect to the TFTP server, use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

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

   ```
   execute reboot
   ```

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

   When one of the following message appears:

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

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

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

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

   Enter G,F,Q,or H:
   ```
7. Type G to get the new firmware image from the TFTP server.

   The following message appears:

   ```
   Enter TFTP server address [192.168.1.168]:
   ```
8. Type the address of the TFTP server and press Enter.

   The following message appears:

   ```
   Enter Local Address [192.168.1.188]:
   ```
9. Type an IP address that can be used by the FortiGate unit to connect to the FTP server.

   The IP address can be any IP address that is valid for the network the interface is connected to. Make sure you do not enter the IP address of another device on this network.

   The following message appears:

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

10 Enter the firmware image file name and press Enter.

The TFTP server uploads the firmware image file to the FortiGate unit and the following message is displayed.

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

11 Type `B`.

The FortiGate unit saves the backup firmware image and restarts. When the FortiGate unit restarts it is running the previously installed firmware version.

Index

FORTINET™

www.fortinet.com