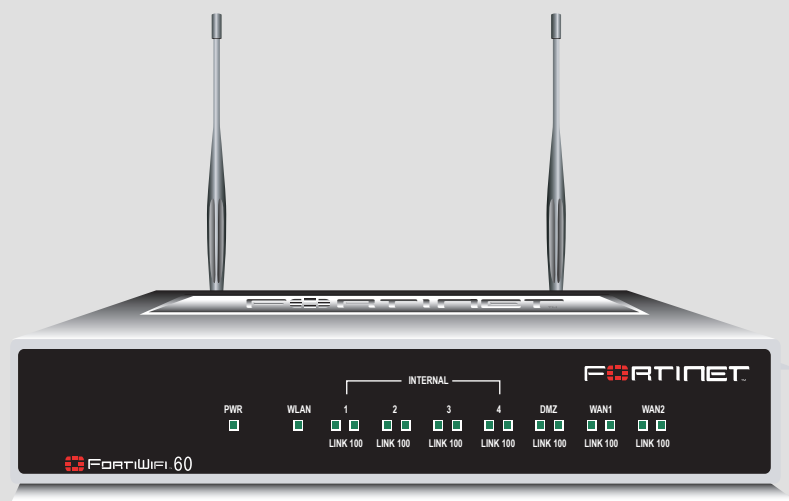


FORTINET™

FortiWiFi 60

Installation and Configuration Guide



Version 2.80 MR8

28 January 2005

01-28008-0030-20050128

© Copyright 2005 Fortinet Inc. All rights reserved.

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

FortiWiFi-60 Installation Guide

Version 2.80 MR8

28 January 2005

01-28008-0030-20050128

Trademarks

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

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

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

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

Table of Contents

Introduction	7
Secure installation, configuration, and management	8
Web-based manager	8
Command line interface	9
Setup wizard	9
Document conventions	9
FortiGate documentation	10
Fortinet Knowledge Center	11
Comments on Fortinet technical documentation.....	11
Related documentation.....	11
FortiManager documentation	11
FortiClient documentation	12
FortiMail documentation.....	12
FortiLog documentation	12
Customer service and technical support.....	12
 Getting started	 15
Package contents	16
Mounting	16
Turning the FortiGate unit power on and off	17
Connecting to the web-based manager	19
Connecting to the command line interface (CLI).....	20
Quick installation using factory defaults.....	21
Factory default FortiGate configuration settings	22
Factory default DHCP server configuration	22
Factory default NAT/Route mode network configuration	23
Factory default Transparent mode network configuration.....	24
Factory default firewall configuration	24
Factory default protection profiles.....	25
Planning the FortiGate configuration	26
NAT/Route mode	27
NAT/Route mode with multiple external network connections.....	28
Transparent mode.....	28
Configuration options	29
Next steps	30
 Using a wireless network	 31
Setting up a wireless network	31
Positioning an Access Point.....	32
Radio Frequency interference.....	32
Using multiple access points.....	33

Wireless Security	34
Wireless Equivalent Privacy (WEP)	34
Wi-Fi Protected Access (WPA)	34
Additional security measures	35
FortiWiFi-60 operation modes.....	35
Access Point mode	35
Client mode	36
Setting up the FortiWiFi-60 as an Access Point.....	37
Log into the web-based manager	37
Set the DHCP settings	38
Set the security options.....	38
Configure the firewall policies	39
NAT/Route mode installation.....	41
Preparing to configure the FortiGate unit in NAT/Route mode	41
DHCP or PPPoE configuration	42
Using the web-based manager	43
Configuring basic settings.....	43
Using the command line interface.....	44
Configuring the FortiGate unit to operate in NAT/Route mode	44
Using the setup wizard.....	47
Starting the setup wizard	48
Connecting the FortiGate unit to the network(s).....	48
Configuring the networks	50
Configuring the Modem interface.....	51
Next steps	51
Transparent mode installation.....	53
Preparing to configure Transparent mode	53
Using the web-based manager	54
Reconnecting to the web-based manager	55
Using the command line interface.....	55
Using the setup wizard.....	57
Reconnecting to the web-based manager	57
Connecting the FortiGate unit to your network	58
Next steps	59
High availability installation.....	61
Priorities of heartbeat device and monitor priorities	61
Configuring FortiGate units for HA operation.....	61
High availability configuration settings	61
Configuring FortiGate units for HA using the web-based manager	63
Configuring FortiGate units for HA using the CLI.....	64

Connecting the cluster to your networks	65
Installing and configuring the cluster.....	67
Configuring the modem interface	69
Selecting a modem mode	69
Redundant mode configuration	69
Standalone mode configuration	70
Configuring modem settings	71
Connecting and disconnecting the modem in Standalone mode.....	72
Defining a Ping Server	73
Dead gateway detection	73
Adding firewall policies for modem connections	74
Index	75

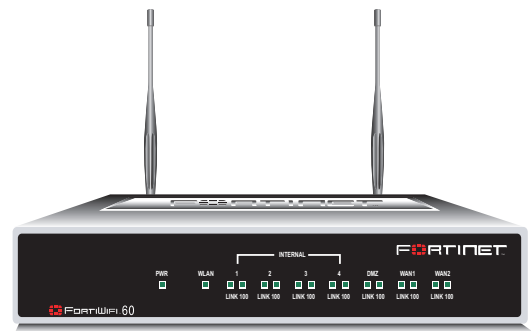
Introduction

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

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

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

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



The FortiWiFi-60 provides a secure, wireless LAN solution that combines mobility and flexibility with the enterprise-class FortiWiFi Antivirus Firewall features. The FortiWiFi is a Wi-Fi certified, wireless LAN transceiver that uses two mini-PCI radios that are IEEE 802.11b and IEEE 802.11g-compliant and that can be upgraded to future radio technologies.

The FortiWiFi serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. FortiWiFi-60 security features include WEP, VPN over the wireless network, and firewall policies that can include user authentication to control access.

Secure installation, configuration, and management

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

- the web-based manager,
- the command line interface (CLI), or
- the setup wizard.

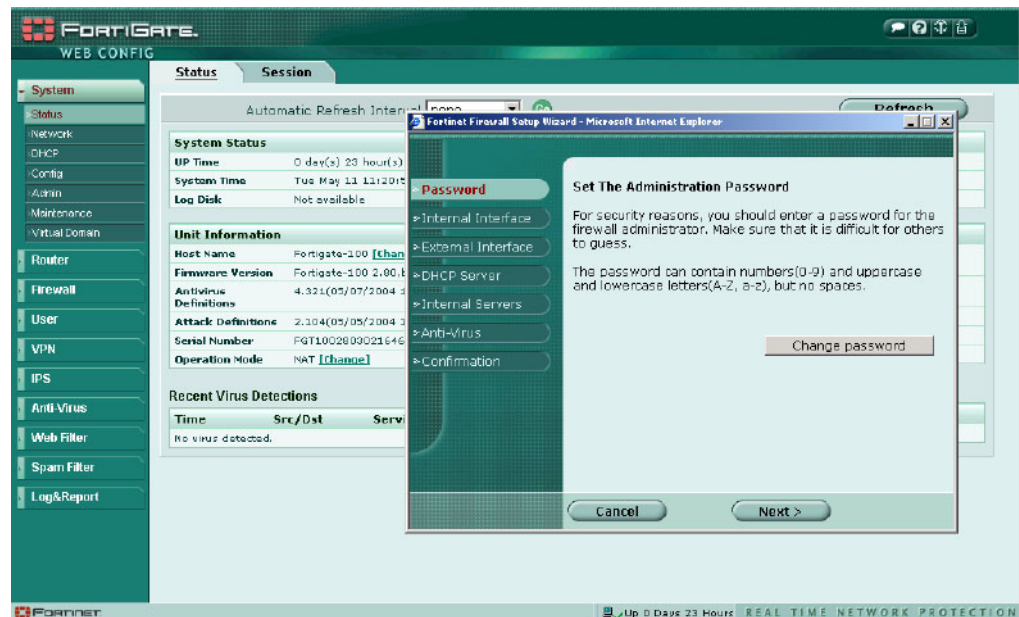
The CLI or the web-based manager can then be used to complete configuration and to perform maintenance and administration.

Web-based manager

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

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

Figure 1: FortiGate web-based manager and setup wizard



Command line interface

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

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

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

Setup wizard

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

Document conventions

This guide uses the following conventions to describe command syntax.

- Angle brackets < > to indicate variables.

For example:

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

You enter:

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

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

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

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

<xxx_ipv4> indicates a dotted decimal IPv4 address.

<xxx_v4mask> indicates a dotted decimal IPv4 netmask.

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

<xxx_ipv6> indicates a dotted decimal IPv6 address.

<xxx_v6mask> indicates a dotted decimal IPv6 netmask.

<xxx_ipv6mask> indicates a dotted decimal IPv6 address followed by a dotted decimal IPv6 netmask.

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

For example:

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

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

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

For example:

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

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

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

For example:

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

You can enter any of the following:

```
set allowaccess ping
```

```
set allowaccess ping https ssh
```

```
set allowaccess https ping ssh
```

```
set allowaccess snmp
```

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

FortiGate documentation

Information about FortiGate products is available from the following guides:

- *FortiGate QuickStart Guide*
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference Guide*

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

- *FortiGate Log Message Reference Guide*

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

- *FortiGate High Availability Guide*

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

- *FortiGate IPS Guide*

Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.

- *FortiGate VPN Guide*

Explains how to configure VPNs using the web-based manager.

Fortinet Knowledge Center

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

Comments on Fortinet technical documentation

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

Related documentation

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

FortiManager documentation

- *FortiManager QuickStart Guide*

Explains how to install the FortiManager Console, set up the FortiManager Server, and configure basic settings.

- *FortiManager System Administration Guide*

Describes how to use the FortiManager System to manage FortiGate devices.

- *FortiManager System online help*

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

FortiClient documentation

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

FortiMail documentation

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

FortiLog documentation

- *FortiLog Administration Guide*
Describes how to install and configure a FortiLog unit to collect FortiGate and FortiMail log files. It also describes how to view FortiGate and FortiMail log files, generate and view log reports, and use the FortiLog unit as a NAS server.
- *FortiLog online help*
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

Customer service and technical support

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

You can also register FortiGate Antivirus Firewalls from <http://support.fortinet.com> and change your registration information at any time.

Fortinet email support is available from the following addresses:

- amer_support@fortinet.com** For customers in the United States, Canada, Mexico, Latin America and South America.
- apac_support@fortinet.com** For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia.
- eu_support@fortinet.com** For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East.

For information on Fortinet telephone support, see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

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



Getting started

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

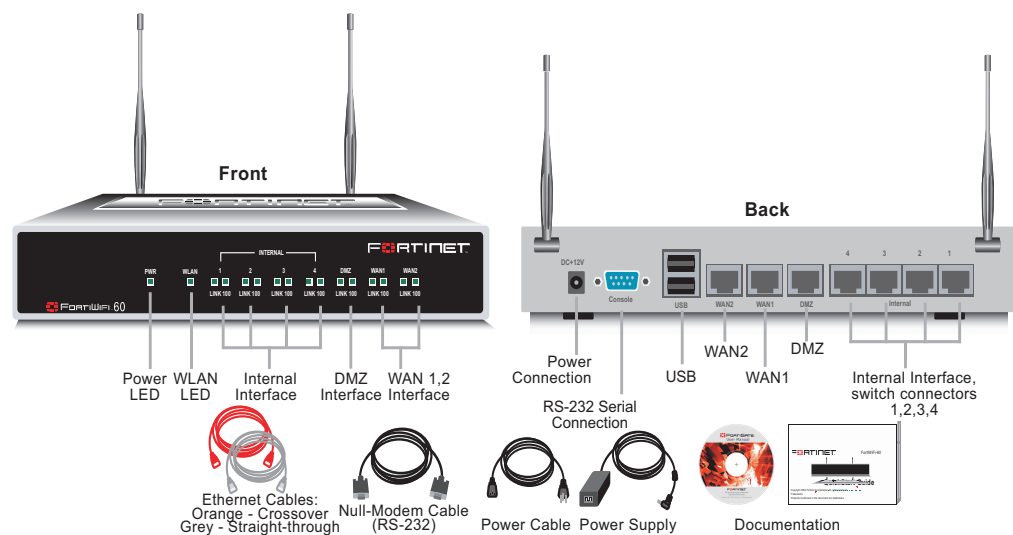
- [Package contents](#)
- [Mounting](#)
- [Turning the FortiGate unit power on and off](#)
- [Connecting to the web-based manager](#)
- [Connecting to the command line interface \(CLI\)](#)
- [Quick installation using factory defaults](#)
- [Factory default FortiGate configuration settings](#)
- [Planning the FortiGate configuration](#)
- [Next steps](#)

Package contents

The FortiWiFi-60 package contains the following items:

- FortiWiFi-60 Antivirus Firewall
- one orange crossover ethernet cable (Fortinet part number CC300248)
- one gray regular ethernet cable (Fortinet part number CC300249)
- null-modem cable (Fortinet part number CC300247)
- FortiWiFi-60 Quick Start Guide
- CD containing the FortiGate user documentation
- one power cable and AC adapter

Figure 2: FortiWiFi-60 package contents



Mounting

The FortiWiFi-60 unit can be installed on any stable surface. Make sure that the unit has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Dimensions

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

Weight

- 1.5 lb. (0.68 kg)

Power requirements

- DC input voltage: 12 V
- DC input current: 3 A

Environmental specifications

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

Wireless Connectivity

- Antenna type: Dual external fixed antenna
- Antenna range: 802.11b/g:2.4GHz
- Antenna Gain: 5dBi

Basic WiFi installation guidelines

Because the FortiWiFi-60 is a radio device, it is susceptible to common causes of interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

- Install the access point in an area where large steel structures such as shelving units, bookcases, and filing cabinets do not block the radio signals to and from the access point.
- Install the access point away from microwave ovens. Microwave ovens operate on the same frequency as the access point and can cause signal interference.

Turning the FortiGate unit power on and off

To power on the FortiGate unit

- 1 Connect the AC adapter to the power connection at the back of the FortiWiFi-60 unit.
- 2 Connect the AC adapter to the power cable.
- 3 Connect the power cable to a power outlet.

The FortiWiFi-60 unit starts. The Power and Status LEDs are on.

Table 1: FortiWiFi-60M LED indicators

LED	State	Description
Power	Green	The FortiGate unit is powered on.
	Off	The FortiGate unit is powered off.
Status	Green	The FortiGate unit is starting up.
	Off	The FortiGate unit is running normally.
Link (Internal DMZ WAN1 WAN2)	Green	The correct cable is in use and the connected equipment has power.
	Flashing Green	Network activity at this interface.
	Off	No link established.
100 (Internal DMZ WAN1 WAN2)	Green	The interface is connected at 100 Mbps.

The FortiWiFi-60 unit starts. The Power and WAN LEDs are on.

Table 2: FortiWiFi-60 LED indicators

LED	State	Description
Power	Green	The FortiGate unit is powered on.
	Off	The FortiGate unit is powered off.
WAN	Green	Traffic on WAN link.
Link (Internal DMZ WAN1 WAN2)	Green	The correct cable is in use and the connected equipment has power.
	Flashing Green	Network activity at this interface.
	Off	No link established.
100 (Internal DMZ WAN1 WAN2)	Green	The interface is connected at 100 Mbps.

To power off the FortiGate unit

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

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

```
execute shutdown
```

- 2 Disconnect the power supply.

Connecting to the web-based manager

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

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

- a computer with an ethernet connection,
- Internet Explorer version 6.0 or higher,
- an ethernet cable.



Note: You can use the web-based manager with recent versions of most popular web browsers. The web-based manager is fully supported for Internet Explorer version 6.0 or higher.

To connect to the web-based manager

- 1 Set the IP address of the computer with an ethernet connection to the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
You can also configure the management computer to obtain an IP address automatically using DHCP. The FortiGate DHCP server assigns the management computer an IP address in the range 192.168.1.1 to 192.168.1.254.
- 2 Using the ethernet cable, 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://).
The FortiGate login is displayed.

Figure 3: FortiGate login

The screenshot shows a web-based login interface. At the top, there is a header with a grid pattern. Below the header, there are two input fields: 'Name:' and 'Password:'. The 'Name:' field is empty. The 'Password:' field is also empty. Below the 'Password:' field, there is a blue button labeled 'Login'.

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

Connecting to the command line interface (CLI)

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

To connect to the FortiGate CLI, you need:

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



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

To connect to the CLI

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

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

- 6 Press Enter to connect to the FortiGate CLI.
The following prompt is displayed:

```
FortiWiFi-60 login:
```

- 7 Type `admin` and press Enter twice.
The following prompt is displayed:

```
Welcome !
```

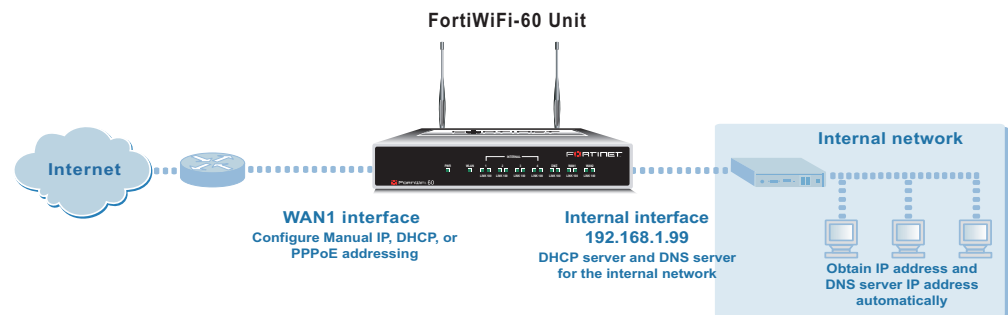
Type `?` to list available commands. For information about how to use the CLI, see the *FortiGate CLI Reference Guide*.

Quick installation using factory defaults

You can quickly set up your FortiGate 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 up to 100 computers in the range 192.168.1.110 –192.168.1.210.

Figure 4: Quick configuration using default settings



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 22](#).

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 WAN1 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 > DNS**.

- 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 30](#).
- 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 30](#).
Go to step 6 if you are not selecting these options.

Factory default FortiGate configuration settings

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

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

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

The factory default 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.

- [Factory default DHCP server configuration](#)
- [Factory default NAT/Route mode network configuration](#)
- [Factory default Transparent mode network configuration](#)
- [Factory default firewall configuration](#)
- [Factory default protection profiles](#)

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 21](#).

Table 3: FortiGate DHCP Server default 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 4 on page 23](#). 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 4 on page 23](#), 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 4: 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	IP: Netmask: Administrative Access:	10.10.10.1 255.255.255.0 HTTPS, Ping
Modem interface	IP: Netmask: Administrative Access:	0.0.0.0 0.0.0.0
WLAN interface	IP: Netmask: Administrative Access:	10.10.80.1 255.255.255.0 Ping

Table 4: Factory default NAT/Route mode network configuration (Continued)

Network Settings	Default Gateway (for default route)	192.168.100.1
	Interface connected to external network (for default route)	wan1
	Default Route A default route consists of a default gateway and the name of the interface connected to the external network (usually the Internet). The default gateway directs all non-local traffic to this interface and to the external network.	
	Primary DNS Server	207.192.200.1
	Secondary DNS Server	207.192.200.129

Factory default Transparent mode network configuration

In Transparent mode, the FortiGate unit has the default network configuration listed in [Table 5](#).

Table 5: Factory default Transparent mode network configuration

Administrator account	User name:	admin
	Password:	(none)
Management IP	IP:	10.10.10.1
	Netmask:	255.255.255.0
DNS	Primary DNS Server:	207.194.200.1
	Secondary DNS Server:	207.194.200.129
Administrative access	Internal	HTTPS, Ping
	WAN1	Ping
	WAN2	Ping
	DMZ	HTTPS, Ping
Administrative access	Internal	HTTPS, Ping
	WAN1	Ping
	WAN2	Ping
	DMZ	HTTPS, 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 6: Default firewall configuration

Configuration setting	Name	Description
Firewall policy	Internal -> Wan1	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 that is controlled by firewall policies. You can use protection profiles to:

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

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

For example, while traffic between internal and external addresses might need strict protection, traffic between trusted internal addresses might need moderate protection. You can configure firewall policies for different traffic services to use the same or different protection profiles.

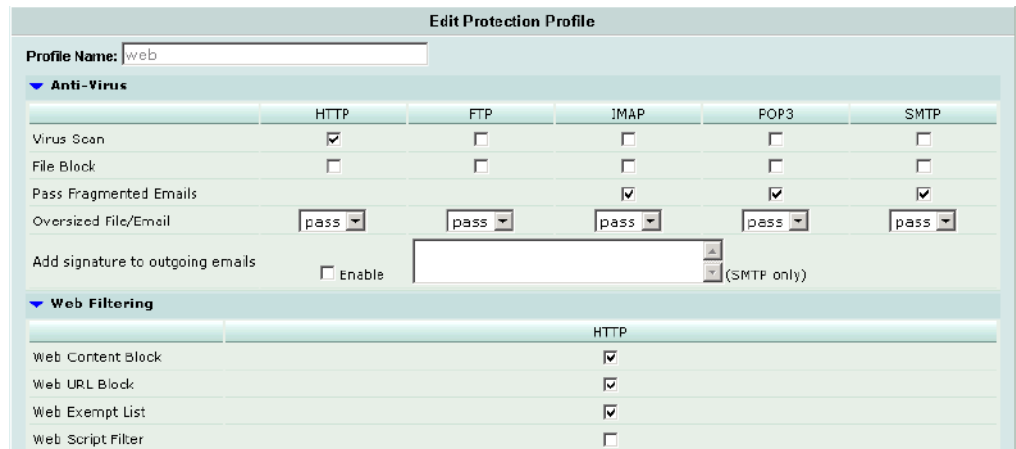
Protection profiles can be added to NAT/Route mode and Transparent mode firewall policies.

The FortiGate unit comes preconfigured with four protection profiles.

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

Figure 5: Web protection profile settings



Planning the FortiGate configuration

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

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

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:

- Internal is the interface to the internal network.
- WAN1 is the default interface to the external network (usually the Internet).
- WAN2 is the redundant interface to the external network.
- DMZ is the interface to the DMZ network.
- Modem is the interface for connecting an external modem to the FortiWiFi-60. See [“Configuring the modem interface” on page 69](#)
- WLAN is the interface to the wireless LAN.

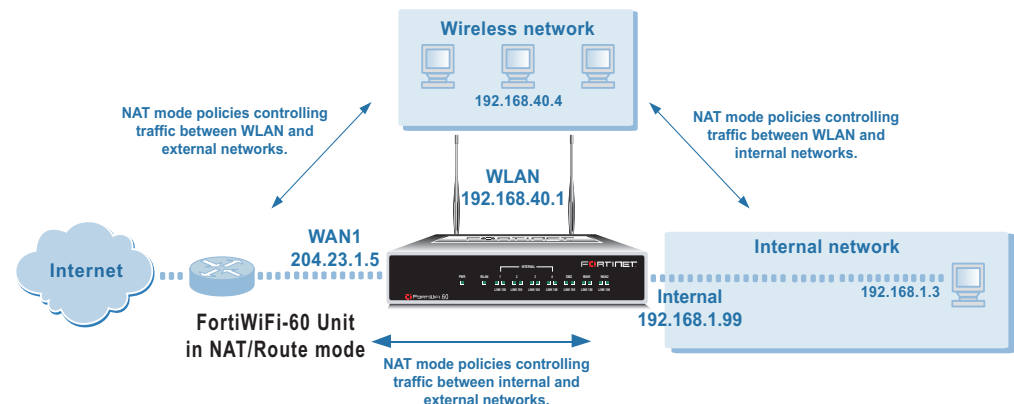
You must configure routing to support the redundant WAN1 and WAN2 internet connections. Routing can be used to automatically redirect connections from an interface if its connection to the external network fails.

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

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

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

Figure 6: Example NAT/Route mode network configuration



NAT/Route mode with multiple external network connections

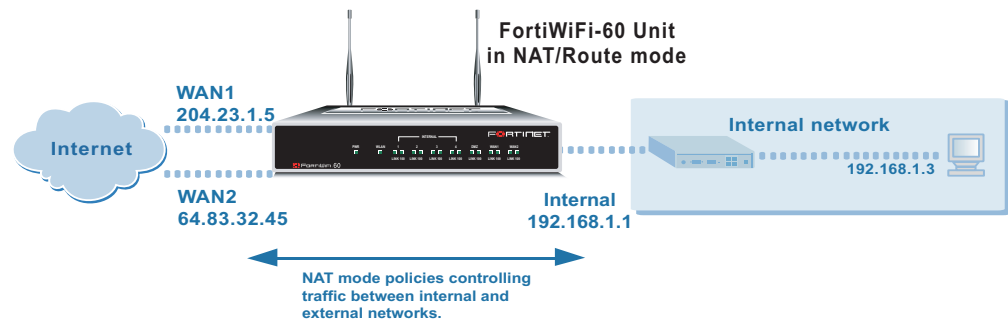
In NAT/Route mode, you can configure the FortiGate unit with multiple redundant connections to the external network (usually the Internet). For example, you could create the following configuration:

- WAN1 is the default interface to the external network (usually the Internet).
- WAN2 is the redundant interface to the external network. You can also use the modem interface as a redundant connection to the external network.
- Internal is the interface to the internal network.

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

Otherwise, security policy configuration is similar to a NAT/Route mode configuration with a single Internet connection. You would create NAT mode firewall policies to control traffic flowing between the internal, private network and the external, public network (usually the Internet). If you have multiple internal networks, such as one or more DMZ networks, in addition to the internal, private network, you can create route mode firewall policies for traffic flowing between them.

Figure 7: Example NAT/Route multiple internet connection configuration

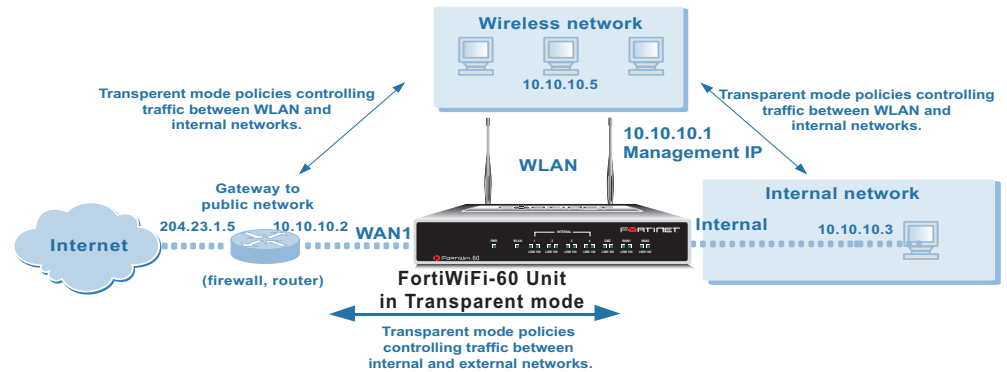


Transparent mode

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

You typically use the FortiGate unit in Transparent mode on a private network behind an existing firewall or behind a router. The FortiGate unit performs firewall functions, IPSec VPN, virus scanning, IPS, web content filtering, and Spam filtering.

Figure 8: Example Transparent mode network configuration



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

- A 4-port switch for connecting the FortiGate internal interface to your internal network segment,
- WAN1 can connect to the external firewall or router,
- DMZ and WAN2 can connect to other network segments,



Note: The modem interface is not available in Transparent mode.

- WLAN can connect to the wireless LAN.

Configuration options

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

Web-based manager and setup wizard

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

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

To connect to the web-based manager you require:

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

CLI

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

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

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

Next steps

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

- If you are going to operate the FortiGate unit in NAT/Route mode, go to [“NAT/Route mode installation” on page 41](#).
- If you are going to operate the FortiGate unit in Transparent mode, go to [“Transparent mode installation” on page 53](#).
- If you are going to operate two or more FortiGate units in HA mode, go to [“High availability installation” on page 61](#).



Using a wireless network

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 that affect the transmission of data “on the air” that you must take into account when setting up a wireless network.

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

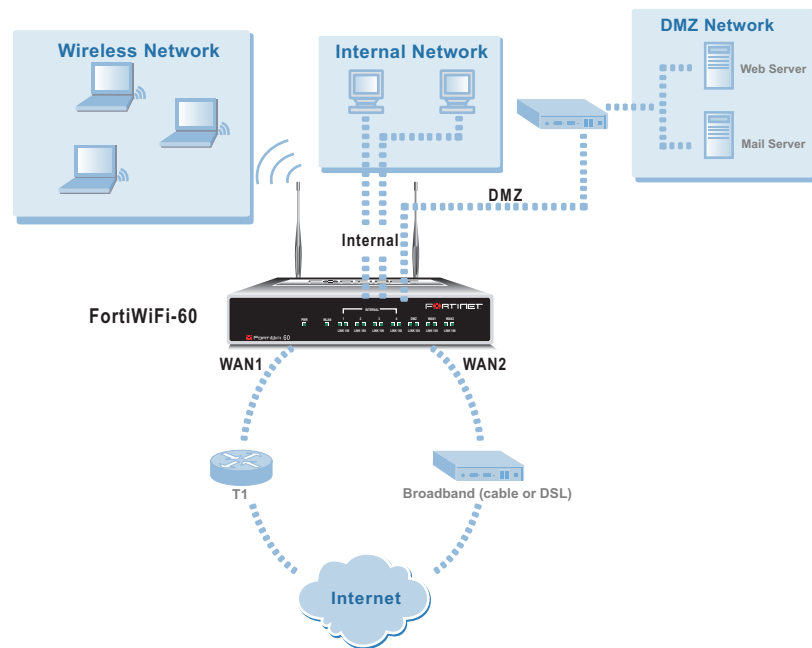
This chapter includes:

- [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 9: 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 signal strength.

Radio Frequency interference

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 2.4GHz cordless phones, microwave ovens and Bluetooth devices can interfere with packet transmission on a wireless network.

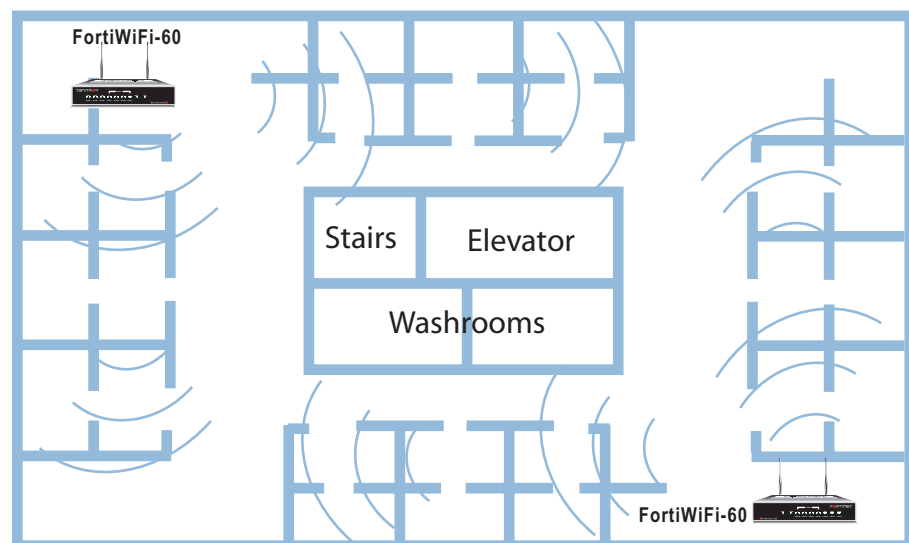
To avoid RF interference:

- 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 the 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 10](#) shows how positioning two FortiWiFi-60 APs within a uniquely shaped office space helps to distribute signals around the area.

Figure 10: Using multiple APs to provide a constant strong signal



This sample office has washrooms, 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, which 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, which generates unique encryption keys automatically with each session. The 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 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 that 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 unit 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.

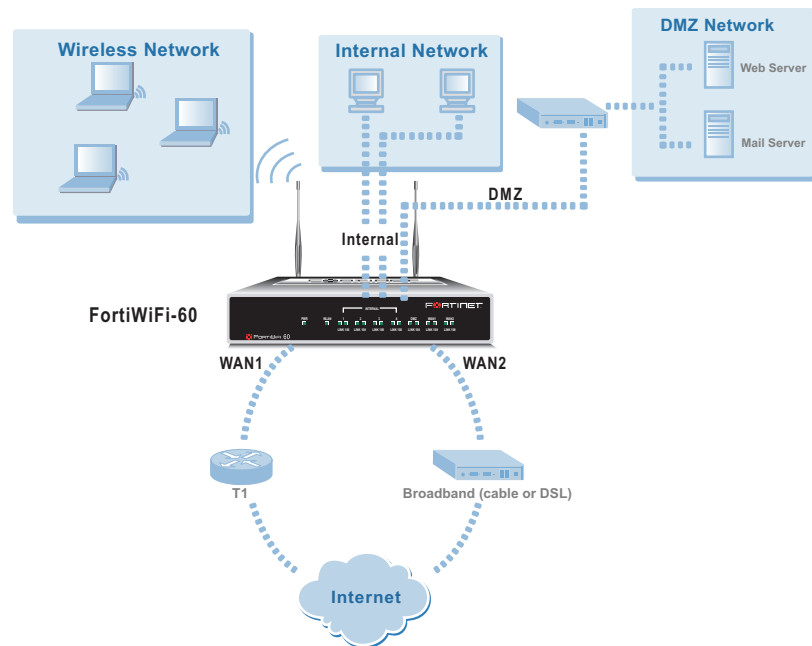
FortiWiFi-60 operation modes

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

Access Point mode

When using the FortiWiFi-60 device 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 the network without the need to connect to it physically. The FortiWiFi-60 device can connect to the internal network and act as a firewall to the internet. Access Point mode is the default mode.

Figure 11: FortiWiFi-60 in Access Point mode

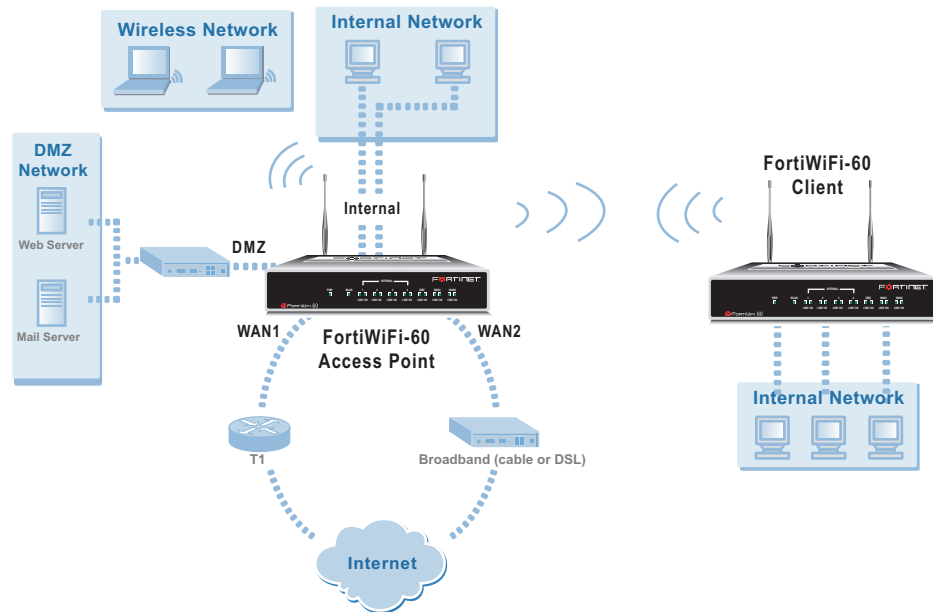


Client mode

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 4 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 12: FortiWiFi-60 in Client mode



Changing the operating mode

To change the wireless operating mode

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

This section contains the following steps:

- [Log into the web-based manager](#)
- [Set the DHCP settings](#)
- [Set the security options](#)
- [Configure the firewall policies](#)

Log into the web-based manager

To set up the FortiWiFi-60 as an access point, you must configure the FortiWiFi-60 unit. For initial setup, use a desktop computer on the internal network with TCP/IP set as DHCP client.

To log into the web-based manager

- 1 Browse to <https://192.168.1.99> (remember to include the “s” in https://).
- 2 Enter `admin` in the Name field.
There is no password by default.
- 3 Select login.

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 to be a DHCP server

- 1 Go to **System > DHCP > Service**.
- 2 Select Edit beside the WLAN interface.
- 3 Select DHCP Server.
- 4 Select OK.

After configuring the FortiWiFi-60 WLAN interface to be a DHCP server, you need to configure the DHCP server settings.

To configure a DHCP server for an interface

- 1 Go to **System > DHCP > Server**.
- 2 Select Create New.
- 3 Enter a name for the DHCP server.
- 4 Select the WLAN interface
- 5 Configure the DHCP server.

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

- 6 Select OK to save the DHCP server configuration.

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**.
- 2 Enter an SSID for your wireless network.
- 3 Set the SSID Broadcast to either enable or disable.
- 4 Select a Security Mode.



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

- 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 Add 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.

Configure the firewall policies

The FortiWiFi-60 unit 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 Authentication.
- 6 Type the user name or group name.
- 7 Select Traffic Shaping
- 8 Configure traffic shaping bandwidth and Traffic Priority settings to meet your requirements.
- 9 Select OK.

NAT/Route mode installation

This chapter describes how to install the FortiGate unit in NAT/Route mode. For information about installing a FortiGate unit in Transparent mode, see [“Transparent mode installation” on page 53](#). For information about installing two or more FortiGate units in HA mode, see [“High availability installation” on page 61](#). For more information about installing the FortiGate unit in NAT/Route mode, see [“Planning the FortiGate configuration” on page 26](#).

This chapter describes:

- [Preparing to configure the FortiGate unit in NAT/Route mode](#)
- [Using the web-based manager](#)
- [Using the command line interface](#)
- [Using the setup wizard](#)
- [Connecting the FortiGate unit to the network\(s\)](#)
- [Configuring the networks](#)
- [Configuring the modem interface](#)
- [Next steps](#)

Preparing to configure the FortiGate unit in NAT/Route mode

Use [Table 7 on page 42](#) to gather the information that you need to customize NAT/Route mode settings.

You can configure the FortiGate unit in several ways:

- the web-based manager GUI is a complete interface for configuring most settings. See [“Using the web-based manager” on page 43](#).
- the command line interface (CLI) is a complete text-based interface for configuring all settings. See [“Using the command line interface” on page 44](#).
- the setup wizard provides easy, fast configuration of the most basic settings to get the unit up and running quickly. See [“Using the setup wizard” on page 47](#).

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

Table 7: NAT/Route mode settings

Administrator Password:		
Internal	IP:	____.____.____.____
	Netmask:	____.____.____.____
WAN1	IP:	____.____.____.____
	Netmask:	____.____.____.____
WAN2	IP:	____.____.____.____
	Netmask:	____.____.____.____
DMZ	IP:	____.____.____.____
	Netmask:	____.____.____.____
WLAN	IP:	____.____.____.____
	Netmask:	____.____.____.____
Network settings	Default Gateway:	____.____.____.____
	Interface connected to external network (usually wan1):	
	A default route consists of a default gateway and the name of the interface connected to the external network (usually the Internet). The default gateway directs all non-local traffic to this interface and to the external network.	
	Primary DNS Server:	____.____.____.____
	Secondary DNS Server:	____.____.____.____

DHCP or PPPoE configuration

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

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

PPPoE requires you to supply a user name and password. In addition, PPPoE unnumbered configurations require you to supply an IP address. Use [Table 8](#) to record the information you require for your PPPoE configuration.

Table 8: PPPoE settings

User name:	
Password:	

Using the web-based manager

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

For information about connecting to the web-based manager, see ["Connecting to the web-based manager" on page 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 > DNS**.
- 2 Enter the IP address of the primary DNS server.
- 3 Enter the IP address of the secondary DNS server.
- 4 Select OK.

To add a default route

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

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

Using the command line interface

You can also configure the FortiGate unit using the command line interface (CLI). For information about connecting to the CLI, see [“Connecting to the command line interface \(CLI\)” on page 20](#).

Configuring the FortiGate unit to operate in NAT/Route mode

Use the information that you gathered in [Table 7 on page 42](#) 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 <psswr>
  end
```

To configure interfaces

- 1 Log in to the CLI.
- 2 Set the IP address and netmask of the internal interface to the internal IP address and netmask that you recorded in [Table 7 on page 42](#). 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 WAN1 interface to the IP address and netmask that you recorded in [Table 7 on page 42](#).

To set the static IP address and netmask, enter:

```
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 <passwr>
  end
```

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

- 5 Confirm that the addresses are correct. Enter:

```
get system interface
```

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

To configure DNS server settings

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

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

Example

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

To add a default route

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

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

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

Example

If the default gateway IP is 204.23.1.2 and this gateway is connected to 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
```

Using the setup wizard

From the web-based manager, you can use the setup wizard to complete the initial configuration of the FortiGate unit. For information about connecting to the web-based manager, see [“Connecting to the web-based manager” on page 19](#).

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

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

[Table 9 on page 47](#) lists the additional settings that you can configure with the setup wizard. See [Table 7 on page 42](#) and [Table 8 on page 42](#) for other settings.

Table 9: Setup wizard settings

Password	Prepare an administrator password.	
Internal Interface	Use the information you gathered in Table 7 on page 42 .	
External Interface	Use the information you gathered in Table 7 on page 42 . The External interface in the setup wizard refers to the WAN1 interface of the FortiGate unit.	
DHCP server	Starting IP:	_____ . _____ . _____ . _____
	Ending IP:	_____ . _____ . _____ . _____
	Netmask:	_____ . _____ . _____ . _____
	Default Gateway:	_____ . _____ . _____ . _____
	DNS IP:	_____ . _____ . _____ . _____
	Your FortiGate firewall contains a DHCP server to automatically set up the addresses of computers on your internal network	
Internal servers	Web Server:	_____ . _____ . _____ . _____
	SMTP Server:	_____ . _____ . _____ . _____
	POP3 Server:	_____ . _____ . _____ . _____
	IMAP Server:	_____ . _____ . _____ . _____
	FTP Server:	_____ . _____ . _____ . _____
	If you provide access from the Internet to a web server, SMTP server, POP3 server IMAP server, or FTP server installed on an internal network, add the IP addresses of the servers here.	

Table 9: Setup wizard settings

Antivirus	High	Create a protection profile that enables virus scanning, file blocking, and blocking of oversized email for HTTP, FTP, IMAP, POP3, and SMTP. Add this protection profile to a default firewall policy.
	Medium	Create a protection profile that enables virus scanning, for HTTP, FTP, IMAP, POP3, and SMTP (recommended). Add this protection profile to a default firewall policy.
	None	Do not configure antivirus protection.
	Select one of these security levels to protect your network from viruses.	

Starting the setup wizard

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

Figure 13: Select the Easy Setup Wizard

- 2 Follow the instructions on the wizard pages and use the information that you gathered in [Table 7 on page 42](#) and [Table 9 on page 47](#) to fill in the wizard fields.
- 3 Select the Next button to step through the wizard pages.
- 4 Confirm the configuration settings, and then select Finish and Close.



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



Note: If you use the setup wizard to configure internal server settings, the FortiGate unit adds port forwarding virtual IPs and firewall policies for each server. For each server located on your internal network the FortiGate unit adds a WAN1->Internal firewall policy.

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-60 unit:

- A 4-port switch for connecting the FortiGate internal interface to your internal network,
- One WAN1 port for connecting to your public switch or router and the Internet,
- One WAN2 port for connecting to a second public switch or router and the Internet for a redundant Internet connection,
- One DMZ port for connecting to a DMZ network.
- Modem is the interface for connecting an external modem to the FortiWiFi-60. See [“Configuring the Modem interface” on page 51](#)
- WLAN is the interface to the wireless LAN.

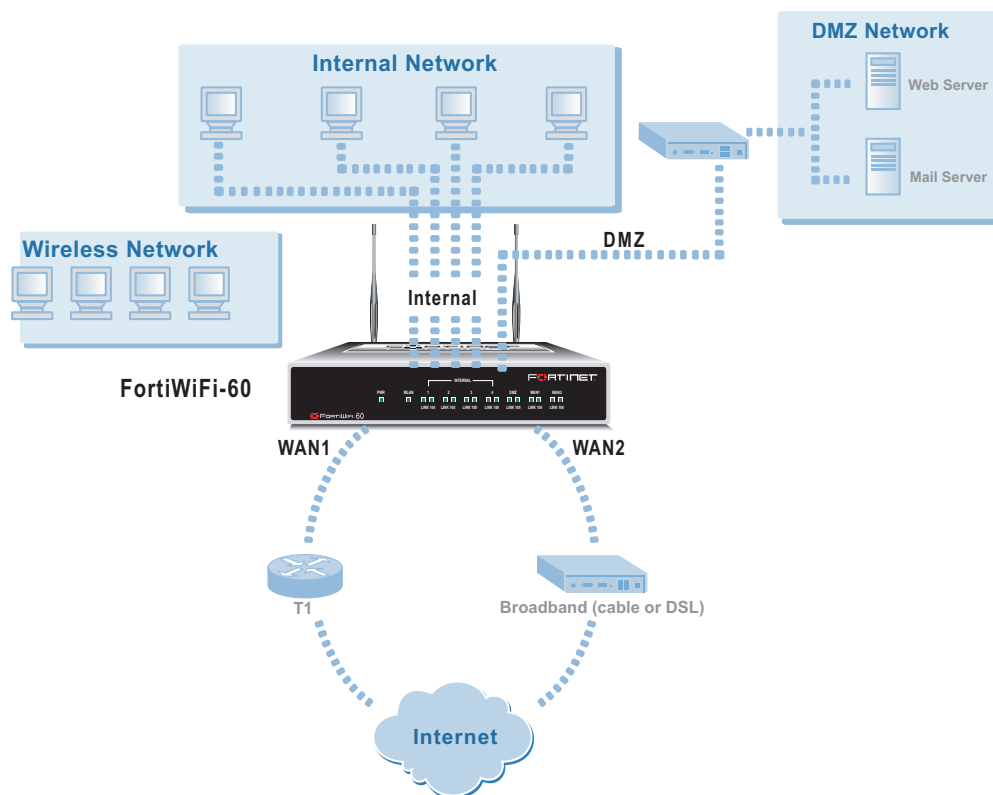


Note: You can also connect the WAN1 and WAN2 interfaces to different Internet connections to provide a redundant connection to the Internet.

To connect the FortiGate unit:

- 1** Connect the Internal interface connectors to PCs and other network devices in your internal network.
The Internal interface functions as a switch, allowing up to four devices to be connected to the internal network and the internal interface.
- 2** Connect the WAN1 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 WAN2 interface to the Internet.
Connect to the public switch or router, usually provided by a different Internet Service Provider. If you are a DSL or cable subscriber, connect the WAN2 interface to the internal or LAN connection of your DSL or cable modem.
- 4** 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 14: 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 FortiGate interface to which they 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 external network, route all packets to the FortiGate WAN1 or WAN 2 interface.

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

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

Configuring the Modem interface

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

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

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

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

Next steps

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

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

To set the date and time

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

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

To use NTP to set the FortiGate date and time

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

To register the FortiGate unit

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

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

To configure virus, attack, and spam definition updates

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

- 1** Go to **System > Maintenance > Update Center**.
- 2** Select Refresh to test the FortiGate unit connectivity with the FortiProtect Distribution Network (FDN).
To be able to connect to the FDN the FortiGate unit default route must point to a network such as the Internet to which a connection to the FDN can be established. If FortiProtect Distribution Network changes to Available, then the FortiGate unit can connect to the FDN.
- 3** Select Scheduled Update and configure a schedule for receiving antivirus and attack definition updates.
- 4** Select Apply.
- 5** You can also select Update Now to receive the latest virus and attack definition updates.

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

Transparent mode installation

This chapter describes how to install a FortiGate unit in Transparent mode. If you want to install the FortiGate unit in NAT/Route mode, see [“NAT/Route mode installation” on page 41](#). If you want to install two or more FortiGate units in HA mode, see [“High availability installation” on page 61](#). For more information about installing the FortiGate unit in Transparent mode, see [“Planning the FortiGate configuration” on page 26](#).

This chapter describes:

- [Preparing to configure Transparent mode](#)
- [Using the web-based manager](#)
- [Using the command line interface](#)
- [Using the setup wizard](#)
- [Connecting the FortiGate unit to your network](#)
- [Next steps](#)

Preparing to configure Transparent mode

Use [Table 10](#) to gather the information that you need to customize Transparent mode settings.

You can configure Transparent mode using four methods:

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

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

Table 10: 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 Select OK.

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

To change the Management IP

- 1 Go to **System > Network > Management**.
- 2 Enter the management IP address and netmask that you recorded in [Table 10 on page 54](#).
- 3 Select access methods and logging for any interfaces as required.
- 4 Select Apply.

To configure DNS server settings

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

To configure the default gateway

- 1 Go to **System > Network > Management**.
- 2 Set Default Gateway to the default gateway IP address that you recorded in [Table 10 on page 54](#).
- 3 Select Apply.

Reconnecting to the web-based manager

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

Using the command line interface

As an alternative to the web-based manager or setup wizard you can begin the initial configuration of the FortiGate unit using the command line interface (CLI). To connect to the CLI, see [“Connecting to the command line interface \(CLI\)” on page 20](#). Use the information that you gathered in [Table 10 on page 54](#) to complete the following procedures.

To change to Transparent mode using the CLI

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

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

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

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

```
Welcome !
```

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

```
get system status
```

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

```
Operation mode: Transparent
```

To configure the management IP address

- 1 Make sure that you are logged into the CLI.
- 2 Set the management IP address and netmask to the IP address and netmask that you recorded in [Table 10 on page 54](#). Enter:

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

Example

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

- 3 Confirm that the address is correct. Enter:

```
get system manageip
```

The CLI lists the management IP address and netmask.

To configure DNS server settings

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

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

Example

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

To configure the default gateway

- 1 Make sure that you are logged into the CLI.
- 2 Set the default route to the default gateway that you recorded in [Table 10 on page 54](#). Enter:

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

Example

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

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

Using the setup wizard

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

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

To start the setup wizard

- 1 Select Easy Setup Wizard (the middle button in the upper-right corner of the web-based manager).
- 2 Use the information that you gathered in [Table 10 on page 54](#) to fill in the wizard fields. Select the Next button to step through the wizard pages.
- 3 Confirm your configuration settings, and then select Finish and Close.

Reconnecting to the web-based manager

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

Connecting the FortiGate unit to your network

When you have completed the initial configuration, you can connect the FortiGate unit between your internal network and the Internet using the Internal and WAN1 interfaces. You can also connect networks to the DMZ interface and the WAN2 interface.

There are seven 10/100Base-TX connectors on the FortiWiFi-60:

- Four Internal ports for connecting to your internal network,
- WAN1 can connect to an external firewall or router.
- DMZ and WAN2 can connect to other network segments.
- WLAN can connect to the wireless LAN.

To connect the FortiGate unit running in Transparent mode:

- 1 Connect the Internal interface connectors to PCs and other network devices in your internal network.

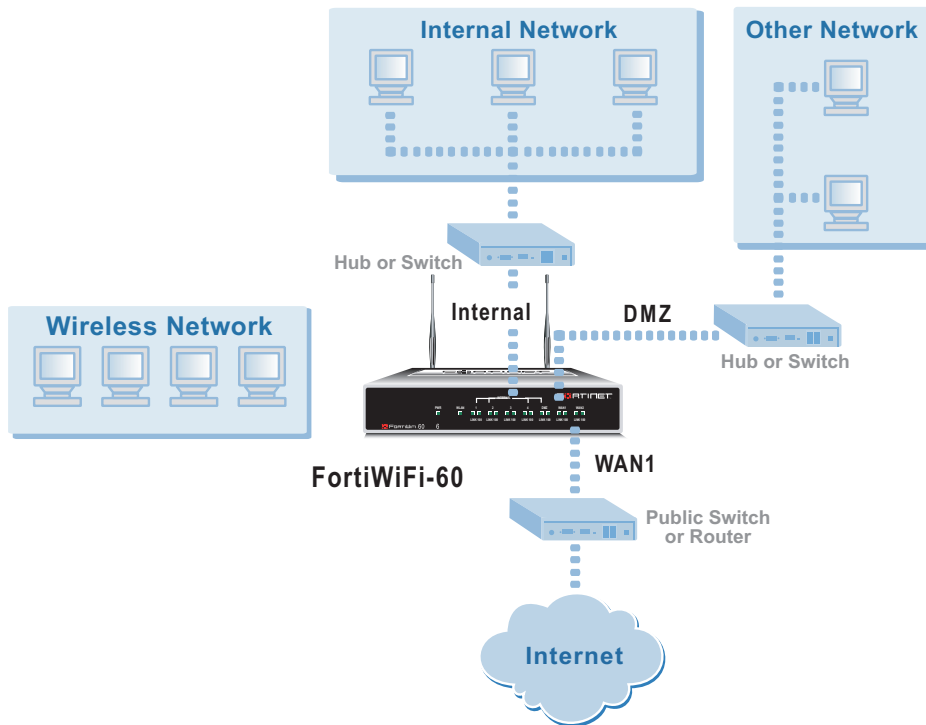
The Internal interface functions as a switch, allowing up to four devices to be connected to the internal network and the internal interface.

- 2 Connect the WAN1 interface to the network segment connected to the external firewall or router.

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 WAN2 and DMZ interfaces to other networks.

Figure 15: FortiWiFi-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.

To set the date and time

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

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

To use NTP to set the FortiGate date and time

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

To register your FortiGate unit

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

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

To configure virus, attack, and spam definition updates

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

- 1** Go to **System > Maintenance > Update Center**.
- 2** Select Refresh to test the FortiGate unit connectivity with the FortiProtect Distribution Network (FDN).
To be able to connect to the FDN the FortiGate unit default route must point to a network such as the Internet to which a connection to the FDN can be established.
If FortiProtect Distribution Network changes to Available, then the FortiGate unit can connect to the FDN.
- 3** Select Scheduled Update and configure a schedule for receiving antivirus and attack definition updates.
- 4** Select Apply.
- 5** You can also select Update Now to receive the latest virus and attack definition updates.

High availability installation

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

- [Configuring FortiGate units for HA operation](#)
- [Connecting the cluster to your networks](#)
- [Installing and configuring the cluster](#)

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

Priorities of heartbeat device and monitor priorities

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

Configuring FortiGate units for HA operation

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

- [High availability configuration settings](#)
- [Configuring FortiGate units for HA using the web-based manager](#)
- [Configuring FortiGate units for HA using the CLI](#)

High availability configuration settings

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

Table 11: High availability settings

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

Table 11: High availability settings (Continued)

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

Configuring FortiGate units for HA using the web-based manager

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

To change the FortiGate unit host name

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

- 1 Power on the FortiGate unit to be configured.
- 2 Connect to the web-based manager.
See [“Connecting to the web-based manager” on page 19](#).
- 3 Go to **System > Status**.
- 4 In the Host Name field of the Unit Information section, select Change.
- 5 Type a new host name and select OK.

To configure a FortiGate unit for HA operation

- 1 Go to **System > Config > HA**.
- 2 Select High Availability.
- 3 Select the mode.
- 4 Select a Group ID for the HA cluster.
- 5 If required, change the Unit Priority.
- 6 If required, select Override master.
- 7 Enter and confirm a password for the HA cluster.
- 8 If you are configuring Active-Active HA, select a schedule.
- 9 Select Apply.
The FortiGate unit negotiates to establish an HA cluster. When you select apply you may temporarily lose connectivity with the FortiGate unit as the negotiation takes place.
- 10 If you are configuring a NAT/Route mode cluster, power off the FortiGate unit and then repeat this procedure for all the FortiGate units in the cluster. Once all of the units are configured, continue with [“Connecting the cluster to your networks” on page 65](#).
- 11 If you are configuring a Transparent mode cluster, reconnect to the web-based manager.
You may have to wait a few minutes before you can reconnect.
- 12 Go to **System > Status**.
- 13 Select Change to Transparent Mode and select OK to switch the FortiGate unit to Transparent mode.
- 14 Allow the FortiGate unit to restart in Transparent mode and then power off the FortiGate unit.
- 15 Repeat this procedure for all of the FortiGate units in the cluster.
- 16 Once all units are configured, continue with [“Connecting the cluster to your networks” on page 65](#).

Configuring FortiGate units for HA using the CLI

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

To change the FortiGate unit host name

- 1 Power on the FortiGate unit to be configured.
- 2 Connect to the CLI.
See [“Connecting to the command line interface \(CLI\)” on page 20](#).
- 3 Change the host name.

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

To configure the FortiGate unit for HA operation

1 Configure HA settings.

Use the following command to:

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

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

The FortiGate unit negotiates to establish an HA cluster.

- 2** If you are configuring a NAT/Route mode cluster, power off the FortiGate unit and then repeat this procedure for all the FortiGate units in the cluster. Once all of the units are configured, continue with [“Connecting the cluster to your networks” on page 65](#).
- 3** If you are configuring a Transparent mode cluster, switch the FortiGate unit to Transparent mode.

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

- 4** Allow the FortiGate unit to restart in Transparent mode and then power off the FortiGate unit.
- 5** Repeat this procedure for all of the FortiGate units in the cluster then continue with [“Connecting the cluster to your networks” on page 65](#).

Connecting the cluster to your networks

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

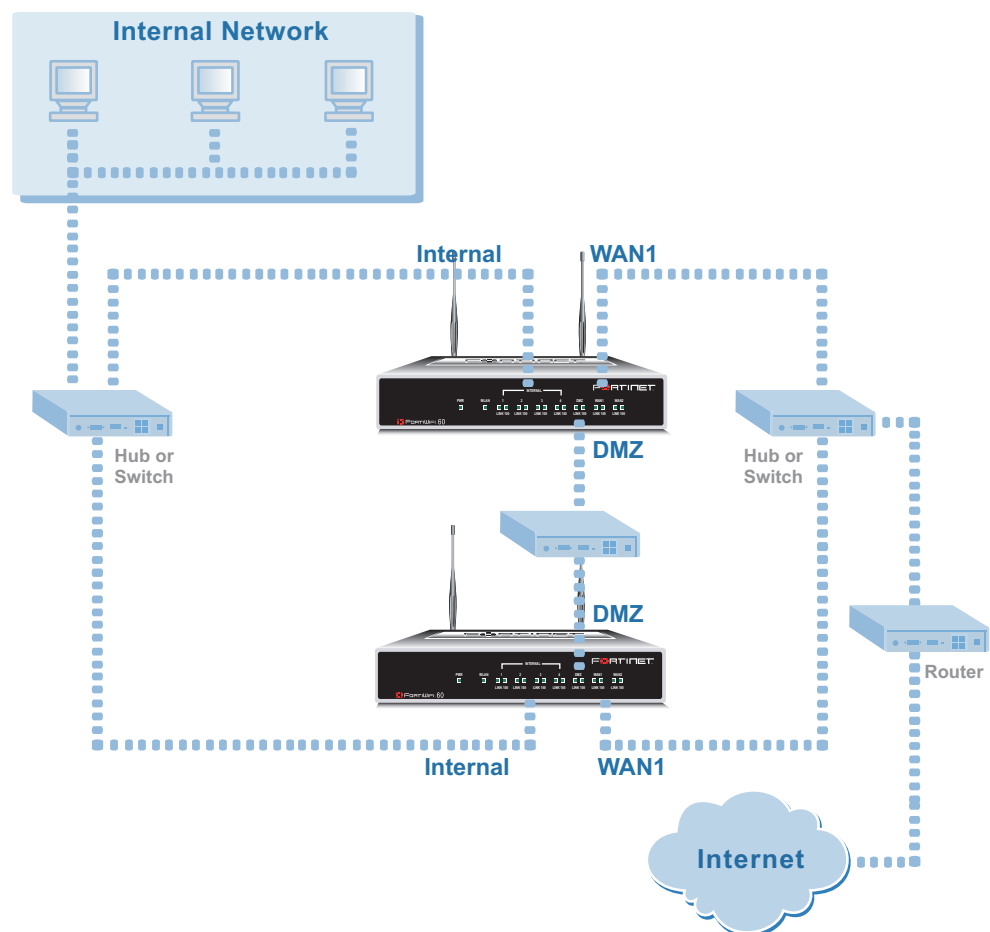
Fortinet recommends using switches for all cluster connections for the best performance.

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

To connect the cluster

- 1 Connect the cluster units:
 - Connect the internal interfaces of each FortiGate unit to a switch or hub connected to your internal network.
 - Connect the WAN1 interfaces of each FortiGate unit to a switch or hub connected to your external network.
 - Connect the DMZ interfaces of the FortiGate units to another switch or hub. By default the DMZ interfaces are used for HA heartbeat communications. These interfaces should be connected together for the HA cluster to function.
 - Optionally connect the WAN2 interface of each FortiGate unit to a switch or hub connected a second external network.

Figure 16: HA network configuration



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

Installing and configuring the cluster

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

- If you are installing a NAT/Route mode cluster, use the information in [“NAT/Route mode installation” on page 41](#) to install the cluster on your network
- If you are installing a Transparent mode cluster, use the information in [“Transparent mode installation” on page 53](#) to install the cluster on your network.

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

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

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

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

Configuring the modem interface

The FortiWiFi-60 includes the option of an external modem for use as either a redundant interface or a standalone 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 standalone 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 dialup accounts until the modem connects to an ISP.

This chapter describes:

- [Selecting a modem mode](#)
- [Configuring modem settings](#)
- [Connecting and disconnecting the modem in Standalone mode](#)
- [Defining a Ping Server](#)
- [Adding firewall policies for modem connections](#)

Selecting a modem mode

The external modem, when connected to the FortiWiFi-60 can work in one of two modes, depending on your requirements:

- redundant mode
- standalone mode.

Redundant mode configuration

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



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

To configure backup mode To configure a redundant modem connection

- 1 Go to **System > Network > Modem**.
- 2 Select Redundant for the mode.
- 3 From the Redundant for list, select the ethernet interface that you want the modem to back up.
- 4 Configure other modem settings as required.
[“Configuring modem settings” on page 71.](#)
- 5 Configure a ping server for the ethernet interface selected in step 3.
See [“Defining a Ping Server” on page 73.](#)
- 6 Configure firewall policies for connections to the modem interface.
See [“Adding firewall policies for modem connections” on page 74.](#)

Standalone mode configuration

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

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

In standalone mode the modem interface replaces the WAN1 or WAN2 ethernet interface. When configuring the modem, you must set Redundant for to the name of the ethernet interface that the modem interface replaces. You must also configure firewall policies for connections between the modem interface and other FortiGate interfaces.



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



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

To operate in standalone mode

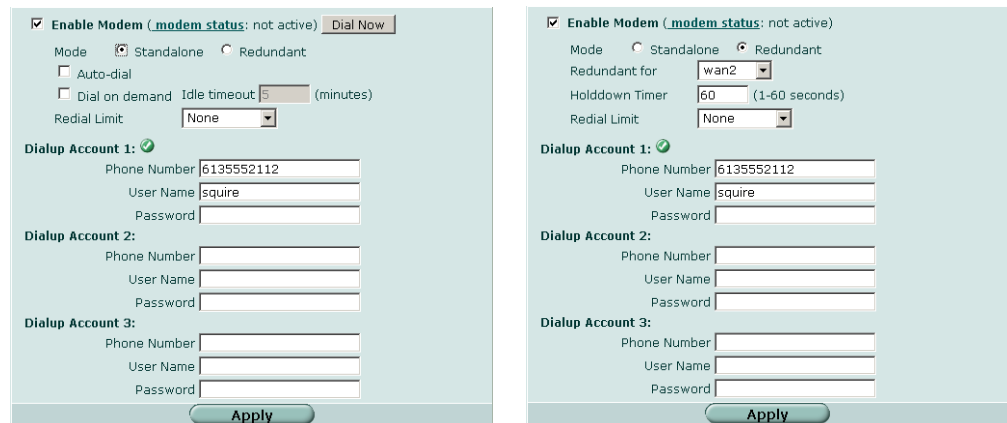
- 1 Go to **System > Network > Modem**.
- 2 From the Redundant for list, select the ethernet interface that the modem is replacing.

- 3 Configure other modem settings as required.
See [“Configuring modem settings” on page 71](#).
Make sure there is correct information in one or more Dialup Accounts.
- 4 Configure firewall policies for connections to the modem interface.
See [“Adding firewall policies for modem connections” on page 74](#).
- 5 Select Dial Up.
The FortiGate unit initiates dialing into each dialup account in turn until the modem connects to an ISP.

Configuring modem settings

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

Figure 17: Modem settings (Standalone and Redundant)



- Enable Modem or Enable USB Modem** Select to enable the FortiGate modem. Depending on the model, the modem is internal or it is a USB-connected external modem.
- Modem status** The modem status shows one of: "not active", "connecting", "connected", "disconnecting" or "hung up" (Standalone mode only).
- Dial Now/Hang Up** (Standalone mode only) Select Dial Now to manually connect to a dialup account. If the modem is connected, you can select Hang Up to manually disconnect the modem.
- Mode** Select Standalone or Redundant mode. In Standalone mode, the modem is an independent interface. In Redundant mode, the modem is a backup facility for a selected Ethernet interface.
- Auto-dial** (Standalone 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 for which the modem provides backup service.

Dial on demand	(Standalone 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	(Standalone 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) that the FortiGate unit waits before switching from the modem interface to the primary interface, after the primary interface has been restored. The default is 1 second. Configure a higher value if you find the FortiGate unit switching repeatedly between the primary interface and the modem interface.
Redial Limit	The maximum number of times (1-10) that the FortiGate unit modem attempts to reconnect to the ISP if the connection fails. The default redial limit is 1. Select None to have no limit on redial attempts.
Dialup Account	Configure up to three dialup 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 following dialup connection settings:
- 4 Enter the following Dialup Account 1 settings:
- 5 If you have multiple dialup accounts, enter Phone Number, User Name, and Password for Dialup Account 2 and Dialup Account 3.
- 6 Select Apply.

Connecting and disconnecting the modem in Standalone mode

To connect to a dialup account

- 1 Go to **System > Network > Modem**.
- 2 Select Enable Modem.
- 3 Make sure there is correct information in one or more Dialup Accounts.
- 4 Select Apply if you make any configuration changes.

5 Select Dial Now.

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

Modem status is one of the following:

not active The modem interface is not connected to the ISP.

active The modem interface is attempting to connect to the ISP, or is connected to the ISP.

A green check mark indicates the active dialup account.

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

To disconnect the modem

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

- 1 Go to **System > Network > Modem**.
- 2 Select Hang Up if you want to disconnect from the dialup account.

Defining 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 that 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, above.

To modify the dead gateway detection settings

- 1 Go to **System > Config > Options**.
- 2 For Detection Interval, type a number in seconds to specify how often the FortiGate unit tests the connection to the ping target.

- 3 For Fail-over Detection, type a number of times that the connection test fails before the FortiGate unit assumes that the gateway is no longer functioning.
- 4 Select Apply.

Adding 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*.

Index

A

- access point
 - mode 35
 - multiple 33
 - positioning 32
- auto-dial 71
- avoiding radio interference 32

B

- broadcasting a SSID 35

C

- CLI 9
 - configuring IP addresses 55
 - configuring NAT/Route mode 44
 - connecting to 20
- client mode 36
- cluster
 - connecting 65, 67
- command line interface 9
- configuring redundant mode 69
- configuring standalone mode 70
- connect
 - cluster 65, 67
- connecting
 - to network 48, 58
 - web-based manager 19
- customer service 12

D

- default gateway
 - configuring (Transparent mode) 56
- default route 23
- dial now 71
- dial on demand 72

E

- encryption 34
 - WEP 34
 - WPA 34
- environmental specifications 17

F

- firewall policies 39
 - modem 74
- firewall setup wizard 8, 43, 47, 54, 57
 - starting 43, 48, 54, 57
- Fortinet customer service 12

H

- HA
 - configuring FortiGate units for HA operation 61
 - connecting an HA cluster 65, 67
- hang up 71
- High availability 61
- holddown timer 72
- HTTPS 8

I

- interference 32
- internal network
 - configuring 50
- IP addresses
 - configuring from the CLI 55

L

- lease duration
 - DHCP 23

M

- MAC address filtering 35
- management IP address
 - transparent mode 56
- modem
 - adding firewall policies 74
 - configuring settings 71
 - redundant mode 69
 - standalone mode 69, 70
- multiple access points 33

N

- NAT/Route mode
 - configuration from the CLI 44

NTP 51, 59
NTP server 51, 59

P

ping server 73
positioning an access point 32
power requirements 16
powering on 17

R

radio frequency interference 32
RADIUS server 34
redial limit 72
redundant mode
 configuring 69
 modem 69

S

security 34
 MAC address filtering 35
 SSID 35
set time 51, 59
setup wizard 43, 47, 54, 57
 starting 43, 48, 54, 57
SSID 35
 broadcasting 35

standalone mode
 configuring 70
 modem 69, 70
starting IP
 DHCP 23
synchronize with NTP server 51, 59

T

technical support 12
time zone 51, 59
Transparent mode
 changing to 55
 configuring the default gateway 56
 management IP address 56

W

web-based manager 8
 connecting to 19
 introduction 8
Wi-Fi Protected Access (WPA) 34
Wireless Equivalent Privacy (WEP) 34
wireless security 34
wizard
 setting up firewall 43, 47, 54, 57
 starting 43, 48, 54, 57