Manualslib.com - The Global Manuals Library

FORTINET FORTIGATE FORTIGATE-200A FIREWALL INSTALL MANUAL

Quick Links

Fortigate-200A

Fortigate-200A

Connecting to the Fortigate Unit

Web-Based Manager

Table of Contents

Table of Contents
FortiGate-200A
FortiGate-300A
FortiGate-400A
FortiGate-500A
Register your FortiGate unit
FortiGuard Subscription Services
FortiClient
FortiMail
FortiAnalyzer
FortiReporter
FortiBridge
FortiManager
Document conventions
Typographic conventions
Fortinet documentation CDs
Fortinet Knowledge Center
Comments on Fortinet technical documentation
FortiGate-200A
Mounting
FortiGate-300A
Mounting
FortiGate-400A
Mounting
FortiGate-500A
Mounting
Air Flow
Mechanical Loading
Powering off the FortiGate unit
Web-based manager

Front control buttons and LCD
Command line interface
Connecting to the web-based manager
System Dashboard
Command line interface
Connecting to the CLI
Using the front control buttons and LCD
Factory default NAT/Route mode network configuration
Factory default Transparent mode network configuration
Factory default firewall configuration
Factory default protection profiles
Restoring the default settings using the web-based manager
Restoring the default settings using the CLI
NAT/Route mode
NAT/Route mode with multiple external network connections
Transparent mode
Preparing to configure the FortiGate unit in NAT/Route mode
DHCP or PPPoE configuration
Using the web-based manager
Configuring basic settings
Adding a default route
Verifying the web-based manager configuration
Verify the connection
Using the front control buttons and LCD
Adding a default gateway using the front control buttons and LCD
Verifying the front control buttons and LCD
Verify the connection
Using the command line interface
Configuring the FortiGate unit to operate in NAT/Route mode
Adding a default route
Verify the connection
Connecting the FortiGate unit to the network(s)
Configuring the networks

Preparing to configure Transparent mode
Using the web-based manager
Using the front control buttons and LCD
Adding a default gateway using the front control buttons and LCD
Verifying the front control buttons and LCD
Verify the connection
Using the command line interface
Reconnecting to the web-based manager
Connecting the FortiGate unit to your network
Verify the connection
Set the date and time
Updating antivirus and IPS signatures
Updating antivirus and IPS signatures from the web-based manager
Updating the IPS signatures from the CLI
Scheduling antivirus and IPS updates
Adding an override server
Upgrading the firmware using the web-based manager
Upgrading the firmware using the CLI
Reverting to a previous firmware version using the web-based manager
Reverting to a previous firmware version using the CLI
Restoring the previous configuration
Backup and Restore from the FortiUSB key
Using the USB Auto-Install feature
Additional CLI Commands for the FortiUSB key
get system status
Other ManualsLib Projects

FortiGate-200A, FortiGate-300A, FortiGate-400A, and FortiGate-500A FortiOS 3.0 MR4

FORTINET™

www.fortinet.com

Downloaded from www.Manualslib.com manuals search engine

FortiGate-200A, FortiGate-300A, FortiGate-400A, and FortiGate-500A Install Guide
FortiOS 3.0 MR4
12 July 2007
01-30004-0268-20070712

© Copyright 2007 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.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Caution: Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions.

Downloaded from www.Manualslib.com manuals search engine

Contents

Contents 3

Introduction 7

About the FortiGate units 7

FortiGate-200A 7

FortiGate-300A 7

FortiGate-400A 8

FortiGate-500A 8

Register your FortiGate unit 8

Fortinet Family Products 8

FortiGuard Subscription Services 8

FortiClient 9

FortiMail 9

FortiAnalyzer 9

FortiReporter 10

FortiBridge 10

FortiManager 10

About this document 10

Document conventions 10

Typographic conventions 11

Fortinet documentation 11

Fortinet documentation CDs 12

Fortinet Knowledge Center 12

Comments on Fortinet technical documentation 13

Customer service and technical support 13

Installing the FortiGate unit 15

Package Contents 15

FortiGate-200A 15

Mounting 16

FortiGate-300A 16

Mounting 17

FortiGate-400A 17

Mounting 18

FortiGate-500A 18

Mounting 19

Air Flow 19

Mechanical Loading 19

Powering on the FortiGate unit 19

Powering off the FortiGate unit 20

Downloaded from www.Manualslib.com manuals search engine

Connecting to the FortiGate unit 21
Web-based manager 21
Front control buttons and LCD 21
Command line interface 21
Connecting to the web-based manager 21
System Dashboard 23
Command line interface 23
Connecting to the CLI 23
LCD front control buttons 24
Using the front control buttons and LCD 25
Factory defaults 27
Factory default NAT/Route mode network configuration 27
Factory default Transparent mode network configuration 28
Factory default firewall configuration 29
Factory default protection profiles 29
Restoring the default settings 30
Restoring the default settings using the web-based manager 30
Restoring the default settings using the CLI 30
Configuring the FortiGate unit 31
Planning the FortiGate configuration 31
NAT/Route mode 31
NAT/Route mode with multiple external network connections 32
Transparent mode 33
Preventing the public FortiGate interface from responding to ping requests 33
NAT/Route mode installation 34
Preparing to configure the FortiGate unit in NAT/Route mode 34
DHCP or PPPoE configuration 35
Using the web-based manager 35
Configuring basic settings 35
Adding a default route 36
Verifying the web-based manager configuration 37
Verify the connection 37
Using the front control buttons and LCD 37
Adding a default gateway using the front control buttons and LCD 38
Verifying the front control buttons and LCD 38
Verify the connection 38
Using the command line interface 38
Configuring the FortiGate unit to operate in NAT/Route mode 38
Adding a default route 40
Verify the connection 40
Connecting the FortiGate unit to the network(s) 41
Configuring the networks 41

Downloaded from www.Manualslib.com manuals search engine

Transparent mode installation **42**
Preparing to configure Transparent mode 42
Using the web-based manager 43
Using the front control buttons and LCD 43
Adding a default gateway using the front control buttons and LCD 44
Verifying the front control buttons and LCD 44
Verify the connection 44
Using the command line interface 44
Reconnecting to the web-based manager 45
Connecting the FortiGate unit to your network 46
Verify the connection 46
Next Steps **46**
Set the date and time 47
Updating antivirus and IPS signatures 47
Updating antivirus and IPS signatures from the web-based manager 48
Updating the IPS signatures from the CLI 48
Scheduling antivirus and IPS updates 49
Adding an override server 49
FortiGate Firmware **51**
Upgrading to a new firmware version **51**
Upgrading the firmware using the web-based manager 51
Upgrading the firmware using the CLI 52
Reverting to a previous firmware version **53**
Reverting to a previous firmware version using the web-based manager 53
Reverting to a previous firmware version using the CLI 54
Installing firmware images from a system reboot using the CLI **56**
Restoring the previous configuration 58
The FortiUSB key **58**
Backup and Restore from the FortiUSB key 59
Using the USB Auto-Install feature 59
Additional CLI Commands for the FortiUSB key 60
Testing a new firmware image before installing it **61**
Index **65**

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Introduction

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

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

The FortiGate Unified Threat Management System is a dedicated, easily managed security device that delivers a full suite of capabilities, which include:

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

The FortiGate Unified Threat Management System uses Fortinet's Dynamic Threat Prevention System (DTPS™) technology, which leverages breakthrough 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.

About the FortiGate units

The FortiGate-x00A series appliances are designed for larger businesses, and deliver the same enterprise-class network-based antivirus, content filtering, firewall, VPN, and network-based intrusion detection/prevention featured in all FortiGate units.

FortiGate-200A

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

FortiGate-300A

The FortiGate-300A unit meets enterprise-class requirements for performance, availability, and reliability. The FortiGate-300A also support high availability (HA) and includes automatic failover with no session loss, making the FortiGate-300A a good choice for mission critical applications.

Downloaded from www.Manualslib.com manuals search engine

FortiGate-400A

The FortiGate-400A unit meets enterprise-class requirements for performance, availability, and reliability. The FortiGate-400A also supports high availability (HA) and features automatic failover with no session loss, making it the choice for mission critical applications.

FortiGate-500A

The FortiGate-500A unit provides the carrier-class levels of performance and reliability demanded by large enterprises and service providers. With a total of 10 network connections, (including a 4-port LAN switch), and high-availability features with automatic failover with no session loss, the FortiGate-500A is the choice for mission critical applications. The flexibility, reliability, and easy management of the FortiGate-500A makes it a natural choice for managed service offerings.

Register your FortiGate unit

After installing your FortiGate unit, register the unit by visiting http://support.fortinet.com and select Product Registration.

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

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

Fortinet Family Products

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

FortiGuard Subscription Services

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

Downloaded from www.Manualslib.com manuals search engine

FortiGuard Subscription Services includes:

- FortiGuard Antivirus Service
- FortiGuard Intrusion Prevention subscription services (IPS)
- FortiGuard Web Filtering
- FortiGuard Antispam Service
- FortiGuard Premier Service

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

FortiClient

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

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

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

FortiMail

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

FortiAnalyzer

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

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

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

Downloaded from www.Manualslib.com manuals search engine

FortiReporter

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

FortiBridge

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

FortiManager

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

About this document

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

This document contains the following chapters:

- Installing the FortiGate unit – Describes setting up, and powering on a FortiGate unit.
- Factory defaults – Provides the factory defaults settings for the FortiGate unit.
- Configuring the FortiGate unit – Provides an overview of the operating modes of the FortiGate unit and how to integrate the FortiGate unit into your network.
- FortiGate Firmware – Describes how to install, update, restore and test the firmware for the FortiGate device.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.

Downloaded from www.Manualslib.com manuals search engine

- Notes and Cautions are used to provide important information:

Note: Highlights useful additional information.

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

Typographic conventions

FortiGate documentation uses the following typographical conventions:

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

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

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

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

Fortinet documentation

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

The following FortiGate product documentation is available:

- *FortiGate QuickStart Guide*

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

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

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

Downloaded from www.Manualslib.com manuals search engine

- *FortiGate online help*

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

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

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

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

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

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

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

  Explains how to configure a PPTP VPN using the web-based manager.
- *FortiGate Certificate Management User Guide*

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

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

Fortinet documentation CDs

All Fortinet documentation is available from the Fortinet documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation, see the Fortinet Knowledge Center.

Fortinet Knowledge Center

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

Downloaded from www.Manualslib.com manuals search engine

Comments on Fortinet technical documentation

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

Customer service and technical support

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

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

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Installing the FortiGate unit

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

- Package Contents
- Air Flow
- Mechanical Loading
- Powering on the FortiGate unit
- Connecting to the FortiGate unit

Package Contents

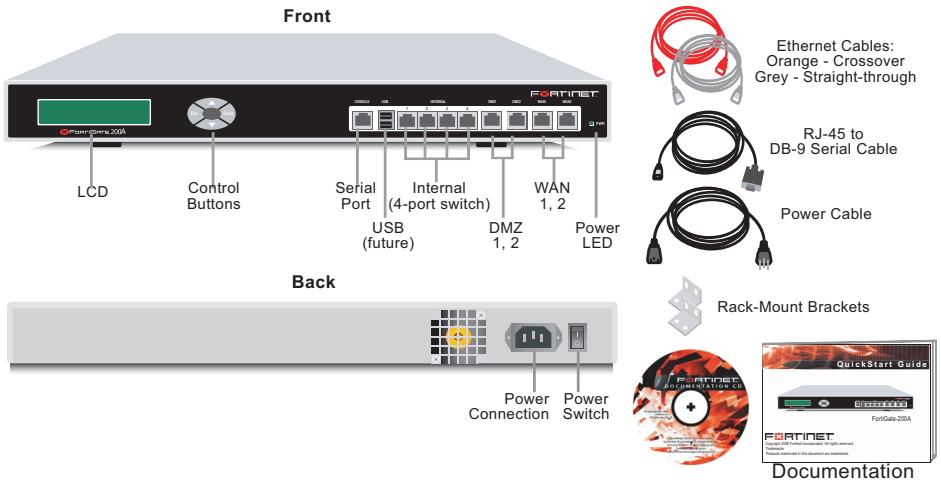
Review the contents of your FortiGate package to ensure all components were included.

FortiGate-200A

The FortiGate-200A package contains the following items:

- FortiGate-200A Unified Threat Management System
- one orange crossover Ethernet cable (CC300248)
- one gray straight-through Ethernet cable (CC300249)
- one RJ-45 to DB-9 serial cable (CC300302)
- two 19-inch rack mount brackets
- one power cable
- FortiGate-200A QuickStart Guide
- Fortinet Tools and Documentation CD

Figure 1: FortiGate-200A package contents



Downloaded from www.Manualslib.com manuals search engine

Mounting

The FortiGate-200A can be installed on any stable surface. The FortiGate-200A unit can also be mounted on a standard 19-inch rack. It requires 1 U of vertical space in the rack.

Table 1: Technical Specifications

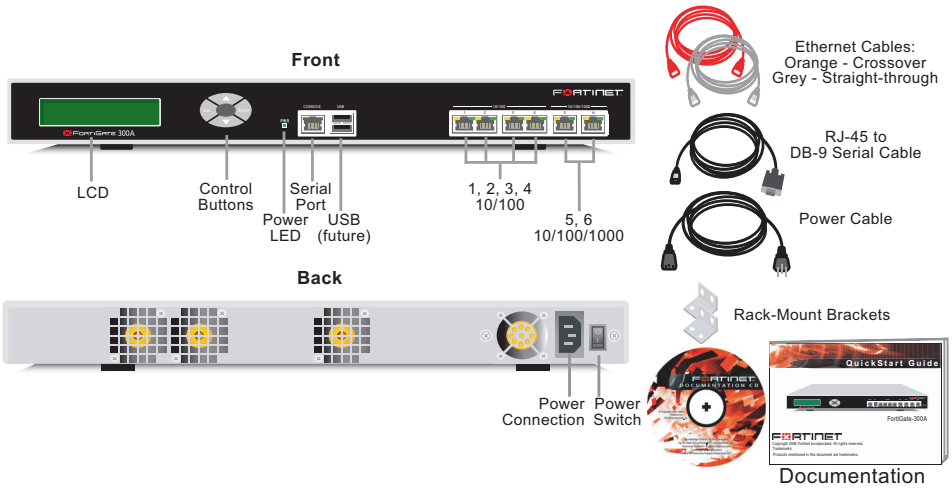
Dimensions	16.8 x 10 x 1.75 in. (42.7 x 25.4 x 4.5 cm.)
Weight	7.3 lb. (3.3 kg)
Power Requirements	Power consumption: 14W AC input voltage: 100 to 240VAC AC input current: 1.6A Frequency: 50 to 60Hz
Environmental specifications	Operating temperature: 32 to 104 F (0 to 40 C) Storage temperature: -13 to 158 F (-25 to 70 C) Humidity: 5 to 95% non-condensing

FortiGate-300A

The FortiGate-300A package contains the following items:

- FortiGate-300A Unified Threat Management System
- one orange crossover Ethernet cable (CC300248)
- one gray straight-through Ethernet cable (CC300249)
- one RJ-45 to DB-9 serial cable (CC300302)
- two 19-inch rack mount brackets
- one power cable
- FortiGate-300A QuickStart Guide
- Fortinet Tools and Documentation CD

Figure 2: FortiGate-300A package contents



Downloaded from www.Manualslib.com manuals search engine

Mounting

The FortiGate-300A can be installed on any stable surface. The FortiGate-300A unit can also be mounted on a standard 19-inch rack. It requires 1 U of vertical space in the rack.

Table 2: Technical Specifications

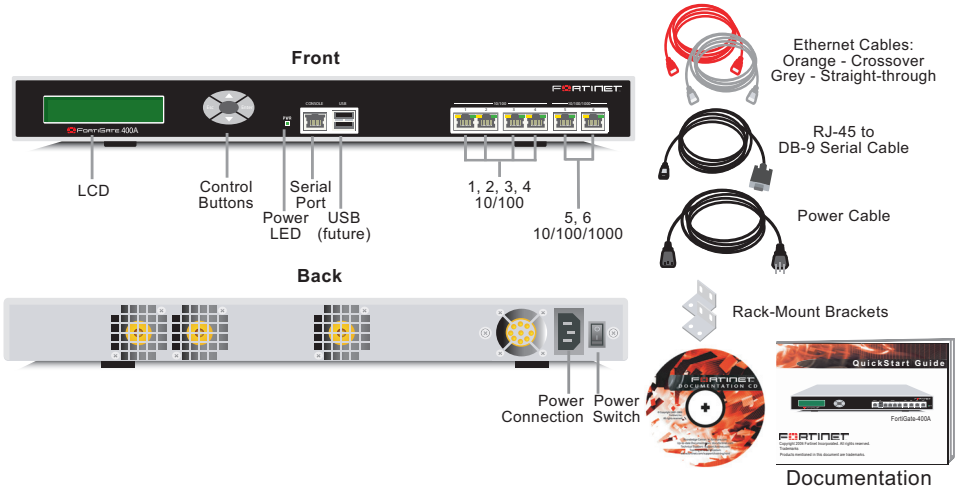
Dimensions	16.8 x 10 x 1.75 in. (42.7 x 25.4 x 4.5 cm.)
Weight	7.3 lb. (3.3 kg)
Power Requirements	Power consumption: 120W AC input voltage: 100 to 240VAC AC input current: 1.6A Frequency: 50 to 60Hz
Environmental Specifications	Operating temperature: 32 to 104 F (0 to 40 C) Storage temperature: -13 to 158 F(-25 to 70 C) Humidity: 5 to 95% non-condensing

FortiGate-400A

The FortiGate-400A package contains the following items:

- FortiGate-400A Unified Threat Management System
- one orange crossover Ethernet cable (CC300248)
- one gray straight-through Ethernet cable (CC300249)
- one RJ-45 to DB-9 serial cable (CC300302)
- two 19-inch rack mount brackets
- one power cable
- FortiGate-400A QuickStart Guide
- Fortinet Tools and Documentation CD

Figure 3: FortiGate-400A package contents



Downloaded from www.Manualslib.com manuals search engine

Mounting

The FortiGate-400A can be installed on any stable surface. The FortiGate-400A unit can also be mounted on a standard 19-inch rack. It requires 1 U of vertical space in the rack.

Table 3: Technical Specifications

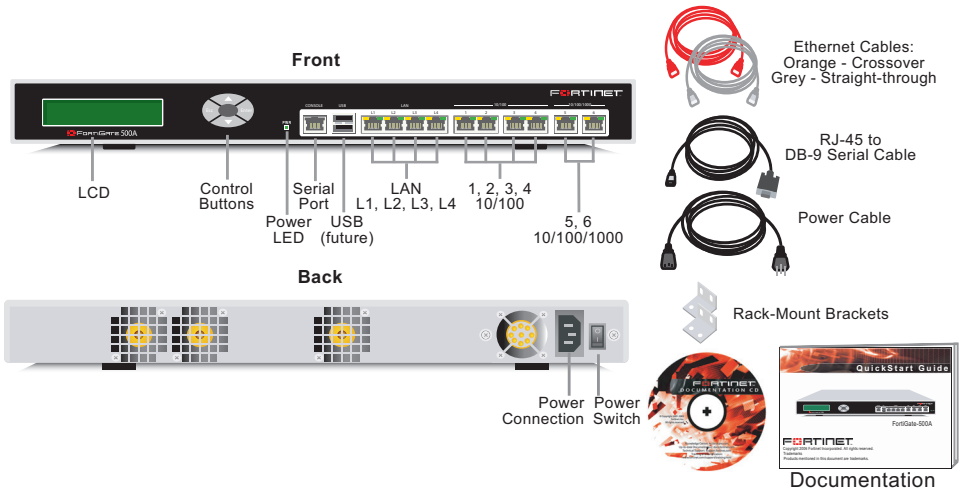
Dimensions	16.8 x 10 x 1.75 in. (42.7 x 25.4 x 4.5 cm.)
Weight	7.3 lb. (3.3 kg)
Power Requirements	Power consumption: 130W AC input voltage: 100 to 240VAC AC input current: 1.6A Frequency: 50 to 60Hz
Environmental Specifications	Operating temperature: 32 to 104 F (0 to 40 C) Storage temperature: -13 to 158 F(-25 to 70 C) Humidity: 5 to 95% non-condensing

FortiGate-500A

The FortiGate-500A package contains the following items:

- FortiGate-500A Unified Threat Management System
- one orange crossover Ethernet cable (CC300248)
- one gray straight-through Ethernet cable (CC300249)
- one RJ-45 to DB-9 serial cable (CC300302)
- two 19-inch rack mount brackets
- one power cable
- FortiGate-500A QuickStart Guide
- Fortinet Tools and Documentation CD

Figure 4: FortiGate-500A package contents



Downloaded from www.Manualslib.com manuals search engine

Mounting

The FortiGate-500A can be installed on any stable surface. The FortiGate-500A unit can also be mounted on a standard 19-inch rack. It requires 1 U of vertical space in the rack.

Table 4: Technical Specifications

Dimensions	16.8 x 10 x 1.75 in. (42.7 x 25.4 x 4.5 cm.)
Weight	7.3 lb. (3.3 kg)
Power Requirements	Power consumption: 140W AC input voltage: 100 to 240VAC AC input current: 1.6A Frequency: 50 to 60Hz
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

Air Flow

- For rack installation, make sure the amount of air flow required for safe operation of the FortiGate unit is not compromised
- For free-standing installation, make sure the FortiGate unit has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.
- If you install the FortiGate unit in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Make sure the operating ambient temperature does not exceed the manufacturer's maximum rated ambient temperature.

Mechanical Loading

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

Powering on the FortiGate unit

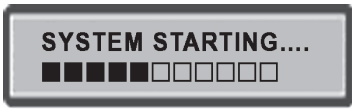
The FortiGate unit has an on/off switch.

To power on the FortiGate unit

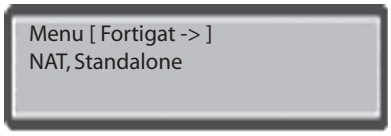
1. Make sure the power switch on the back of the FortiGate unit is turned off.
2. Connect the power cable to the power connection on the back of the FortiGate unit.
3. Connect the power cable to a power outlet.
4. Turn on the power switch.

Downloaded from www.Manualslib.com manuals search engine

After a few seconds, SYSTEM STARTING appears on the LCD.



The main menu setting appears on the LCD when the system is running.



The FortiGate unit starts and the Power LEDs light up.

Table 5: Led indicators

LED	State	Description
Power	Green	The FortiGate unit is powered on.
	Off	The FortiGate unit is powered off.
Status	Flashing Green	The FortiGate unit is starting up.
	Green	The FortiGate unit is running normally.
	Off	The FortiGate unit is powered off.
Internal **External** **WAN1** **WAN2** **DMZ1** **DMZ2** **LAN (L1 -L4)** **1, 2, 3, 4, 5, 6**	Amber	The correct cable is in use, and the connected equipment has power.
	Flashing Amber	Network activity at this interface.
	Green	The interface is connected. • 1, 2, 3, 4, 5 and 6 connect at up to 100 Mbps
	Red	Ports 5 and 6 connect at up to 1000 Mbps.
	Off	No link established.

Powering off the FortiGate unit

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

To power off the FortiGate unit

1. From the web-based manager, go to **System > Status**.
2. In the Unit Operation display, select Shutdown, or from the CLI, enter:

```
execute shutdown
```

3. Turn off the power switch.
4. Disconnect the power supply.

Downloaded from www.Manualslib.com manuals search engine

Connecting to the FortiGate unit

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

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

Web-based manager

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

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

Front control buttons and LCD

You can use the front control buttons and LCD on the FortiGate unit to configure IP addresses, default gateways and switch operating modes. The LCD shows you what mode you are in without having to go to the command line interface (CLI) or the web-based manager. For more information on the front control buttons and LCD, see "LCD front control buttons" on page 24.

Command line interface

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

Connecting to the web-based manager

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

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

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

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

To connect to the web-based manager

1. Set the IP address of the computer with an Ethernet connection to the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
2. Using the crossover cable or the Ethernet hub and cables, connect the internal interface of the FortiGate unit to the computer Ethernet connection.

Downloaded from www.Manualslib.com manuals search engine

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

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

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

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

Figure 5: FortiGate login

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

Downloaded from www.Manualslib.com manuals search engine

System Dashboard

After logging into the web-based manager, the web browser displays the system dashboard. The dashboard provides you with all system status information in one location. For details on the information displayed on the dashboard, see the *FortiGate Administration Guide*.

Command line interface

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

The CLI supports the same configuration and monitoring functionality as the web-based manager. In addition, you can use the CLI for advanced configuration options that are not available from the web-based manager. This guide contains information about basic and advanced CLI commands. For a more complete description about connecting to and using the FortiGate CLI, see the *FortiGate CLI Reference*.

Connecting to the CLI

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

To connect to the FortiGate CLI you require:

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

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

To connect to the CLI

1. Connect the RJ-45 to DB-9 serial cable to the communications port of your computer and to the FortiGate console port.
2. Start HyperTerminal, enter a name for the connection and select OK.
3. Configure HyperTerminal to connect directly to the communications port on your computer and select OK.
4. Select the following port settings and select OK.

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

5. Press Enter to connect to the FortiGate CLI.
   The login prompt appears.

Downloaded from www.Manualslib.com manuals search engine

6 Type `admin` and press Enter twice.
The following prompt is displayed.

```
Welcome!
```

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

LCD front control buttons

You can use the front control buttons and LCD to configure the basic settings on your FortiGate unit. This configuration method provides an easy and fast method to configure your FortiGate unit. You can configure:

- IP addresses
- netmasks
- default gateways
- operating modes
- restore factory default settings

The LCD provides information on the FortiGate unit's operating modes and whether or not it is part of a High Availability (HA) cluster. Figure 6 shows the default LCD main menu setting of a FortiGate unit, operating in NAT/Route mode and not connected to a HA cluster.

Figure 6: Default LCD main menu settings

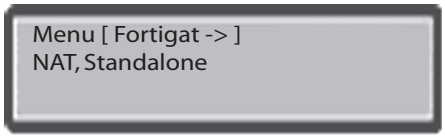


Table 6: LCD main menu definitions

Menu	The menu the LCD currently displays.
[Fortigat ->]	The FortiGate unit's host name.
NAT	The current operational mode of the FortiGate unit.
Standalone	The FortiGate unit is not part of a HA cluster. For more information on standalone mode and HA, see the *FortiGate Administration Guide*.

The front control buttons control how you enter and exit the different menus when configuring the different ports and interfaces. The front control buttons also enables you to increase or decrease each number for configuring IP addresses, default gateway addresses, or netmasks. The following table defines each button and what it does when configuring the basic settings of your FortiGate unit.

Table 7: Front control button definitions

Enter	Enables you to move forward through the configuration process.
Esc	Enables you to move backward, or exit out of the menu you are in.

Downloaded from www.Manualslib.com manuals search engine

Up	Allows you to increase the number for an IP address, default gateway address or netmask.
Down	Allows you to decrease the number for an IP address, default gateway address or netmask.

Using the front control buttons and LCD

When the LCD displays the main menu, you can begin to configure the IP addresses, netmasks, default gateways, and if required, change the operating mode. Use the following procedures as a guide when configuring your FortiGate unit in "Configuring the FortiGate unit" on page 31.

To enter an IP address

1. Press Enter to select the interfaces.
2. Press the up and down buttons to highlight the interface you want to configure an IP address for, and then press Enter.
3. Press Enter for the IP address.
4. Press the up and down buttons to increase or decrease the number.
5. Press Enter to select the number.
6. Repeat steps 4 and 5 for all numbers of the IP address.

   Use the above steps to configure netmasks and default gateways.

To change the operating mode

1. Make sure the LCD displays the main menu setting.
2. Press Enter to select the interfaces.
3. Press the up and down buttons to highlight the menu To Bridge Mode.
4. Press Enter to change to Transparent mode.

   The FortiGate unit changes to Transparent mode. This may take a few minutes.
5. The LCD should display the following:

Figure 7: LCD main menu setting for Transparent mode

To reset to factory defaults

1. Make sure the LCD displays the main menu setting.
2. Press Enter to go to the interfaces.
3. Press the up and down arrows to highlight the menu Restore Defaults.
4. Press Enter.

   The FortiGate unit resets to factory default settings. This may take a few minutes.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Factory defaults

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

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

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

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

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

The following topics are included in this section:

- Factory default NAT/Route mode network configuration
- Factory default Transparent mode network configuration
- Factory default firewall configuration
- Factory default protection profiles
- Restoring the default settings

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 8 on page 28. 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 8 on page 28, 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.

Downloaded from www.Manualslib.com manuals search engine

Table 8: Factory default NAT/Route mode network configuration

Administrator account	User name: Password:	admin (none)
Port 1	IP: Netmask: Administrative Access:	192.168.1.99 255.255.255.0 HTTPS, Ping
Port 2 **WAN1 (200A)**	IP: Netmask: Administrative Access:	192.168.100.99 255.255.255.0 Ping
Port 4 **DMZ (200A)**	IP: Netmask: Administrative Access:	10.10.10.1 255.255.255.0 HTTPS, Ping
Network settings	Default gateway (for default route)	192.168.100.1
	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 the external network.	
	Primary DNS Server Secondary DNS Server	65.39.139.53 65.39.139.63

Factory default Transparent mode network configuration

In Transparent mode, the FortiGate unit has the default network configuration listed in Table 9.

Table 9: Factory default Transparent mode network configuration

Administrator account	User name: Password:	admin (none)
Management IP	IP: Netmask:	0.0.0.0 0.0.0.0
DNS	Primary DNS Server: Secondary DNS Server:	65.39.139.53 65.39.139.63
Administrative access	Port 1 Port 4 DMZ WAN1	HTTPS, Ping Ping HTTPS, Ping Ping

Downloaded from www.Manualslib.com manuals search engine

Factory default firewall configuration

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

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

Table 10: Factory default firewall configuration

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

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

Factory default protection profiles

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

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

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

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

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

Downloaded from www.Manualslib.com manuals search engine

The FortiGate unit comes preconfigured with four protection profiles.

Strict	To apply maximum protection to HTTP, FTP, IMAP, POP3, and SMTP traffic. You may not use the strict protection profile under normal circumstances but it is available if you have problems with viruses and require maximum screening.
Scan	To apply antivirus scanning and file quarantining to HTTP, FTP, IMAP, POP3, and SMTP content traffic.
Web	To apply antivirus scanning and web content blocking to HTTP content traffic. You can add this protection profile to firewall policies that control HTTP traffic.
Unfiltered	To apply no scanning, blocking or IPS. Use if you do not want to apply content protection to content traffic. You can add this protection profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected.

Restoring the default settings

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

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

Restoring the default settings using the web-based manager

To reset the default settings

1. Go to **System > Status**.
2. In the Unit Operation display, select Reset.

Restoring the default settings using the CLI

To reset the default settings, enter the following command:

```
execute factoryreset
```

Note: If you want to restore factory default settings using the front control buttons and LCD, see "LCD front control buttons" on page 24.

Downloaded from www.Manualslib.com manuals search engine

Configuring the FortiGate unit

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

This section includes the following topics:

- Planning the FortiGate configuration
- Preventing the public FortiGate interface from responding to ping requests
- NAT/Route mode installation
- Transparent mode installation
- Next Steps

Planning the FortiGate configuration

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

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

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

NAT/Route mode

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

Table 11: NAT/Route mode network segments

FortiGate Unit	Internal Interface	External Interface	Other
FortiGate-200A	Internal	WAN1 WAN2	DMZ1 DMZ2
FortiGate-300A	Port 2	Port 1	Ports 3, 4, 5, 6
FortiGate-400A	Port 2	Port 2	Ports 3, 4, 5, 6
FortiGate-500A	LAN (L1, L2, L3, L4)	Port 1	Ports 2 to 6

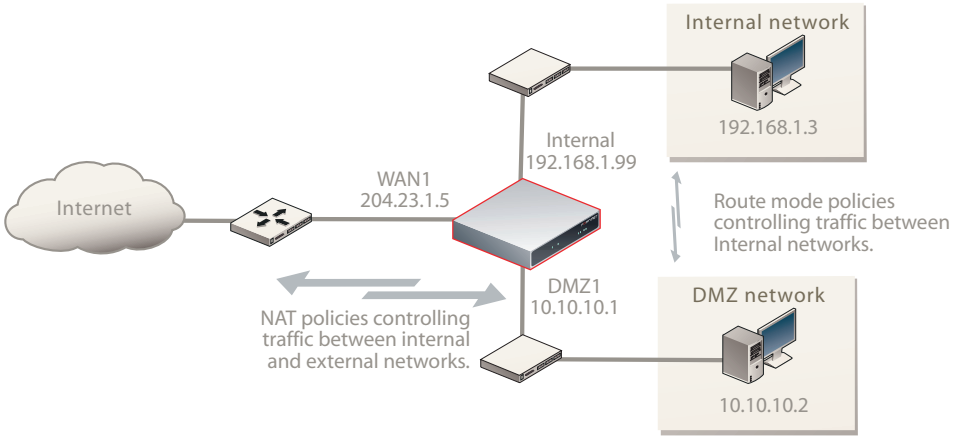
Downloaded from www.Manualslib.com manuals search engine

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

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

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

Figure 8: NAT/Route mode network configuration for a FortiGate-200A.



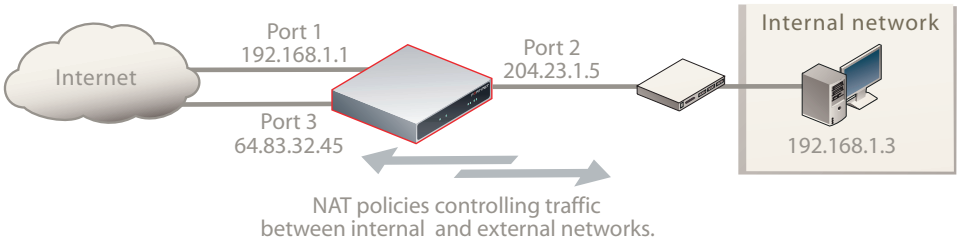
NAT/Route mode with multiple external network connections

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 onfiguration:

- Port 1 is the default interface to the external network (usually the Internet)
- Port 2 is the interface to the internal network
- Port 3 is the redundant interface to the external network

Figure 9: Multiple internet connection configuration for a FortiGate-400A.



Downloaded from www.Manualslib.com manuals search engine

Transparent mode

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

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

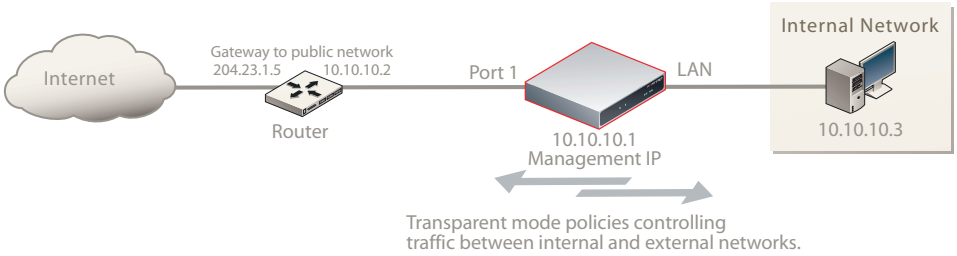
You can connect network segments to the FortiGate unit to control traffic between these network segments. Depending on the FortiGate unit, you can connect up to seven network segments.

Table 12: Transparent mode network segments

FortiGate Unit	Internal Interface	External Interface	Other
FortiGate-200A	4-port switch	WAN1	WAN 2 DMZ1 DMZ2
FortiGate-300A	Port 2	Port 1	Ports 3, 4, 5, 6
FortiGate-400A	Port 2	Port 1	Ports 3, 4, 5, 6
FortiGate-500A	LAN	Port 1	Ports 2 to 6

Note: If you are installing a HA cluster, Port 4 can connect to another FortiGate unit. For example, a FortiGate-300A can connect to another FortiGate-300A through Port 4. This is only available on the FortiGate-300A, FortiGate-400A and FortiGate-500A.

Figure 10: Transparent mode network connections for a FortiGate-500A.



Preventing the public FortiGate interface from responding to ping requests

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

Downloaded from www.Manualslib.com manuals search engine

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

Depending on the FortiGate unit, the default public interface can be the WAN1 interface or Port 2 interface.

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

To disable ping administrative access from the web-based manager

1. Log into the FortiGate web-based manager.
2. Go to **System > Network > Interface**.
3. Choose the external interface and select Edit.
4. Clear the Ping Administrative Access check box.
5. Select OK to save the changes.

To disable ping administrative access from the FortiGate CLI

1. Log into the FortiGate CLI.
2. Disable administrative access to the external interface. Enter:

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

NAT/Route mode installation

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

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

Preparing to configure the FortiGate unit in NAT/Route mode

Use Table 13 on page 35 to gather the information you need to customize NAT/Route mode settings.

You can configure the FortiGate unit in three ways:

- The web-based manager GUI is a complete interface for configuring most settings. See “Using the web-based manager” on page 35.

Downloaded from www.Manualslib.com manuals search engine

- The front control buttons and LCD provide access to basic settings. See "Using the front control buttons and LCD" on page 37.
- The command line interface (CLI) is a complete text-based interface for configuring all settings. See "Using the command line interface" on page 38.

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

Table 13: NAT/Route mode settings

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

DHCP or PPPoE configuration

You can configure any FortiGate interface to acquire its IP address from a DHCP or PPPoE server. Your Internet Service Provider (ISP) may provide 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 14 to record the information you require for your PPPoE configuration.

Table 14: PPPoE settings

User name:	
Password:	

Using the web-based manager

Use the web-based manager for the initial configuration of the FortiGate unit and all FortiGate unit settings. For information about connecting to the web-based manager, see "Connecting to the web-based manager" on page 21.

Configuring basic settings

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

Downloaded from www.Manualslib.com manuals search engine

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 sever settings

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

Adding a default route

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

To add a default route

1 Go to **Router > Static**.
2 If the Static Route table contains a default route (IP and Mask set to 0.0.0.0), select the Delete icon to delete this route.
3 Select Create New.
4 Select Destination IP to 0.0.0.0.

Downloaded from www.Manualslib.com manuals search engine

5 Set Mask to 0.0.0.0.

6 Set Gateway to the default gateway IP address.

7 Set Device to the interface connected to the external network.

8 Select OK.

Verifying the web-based manager configuration

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

Verify the connection

To verify your connection, try the following:

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

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

Using the front control buttons and LCD

Basic settings, including interface IP addresses, netmasks, default gateways, and the FortiGate operating mode can be configured using the front control buttons and LCD on the FortiGate unit. Use the information you recorded in Table 13 on page 35 to complete the following procedure. Start when the main menu setting is displayed on the LCD.

Note: You cannot configure DHCP or PPPoE from the control buttons and LCD on the FortiGate-200A. Instead, you can use the web-based manager or the CLI.

To change the IP address and netmask of an interface

1 Press Enter to display the interface list.

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

3 Press Enter for IP address.

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

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

6 Use the down arrow to highlight Netmask.

7 Press Enter and change the Netmask.

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

9 Press Esc to return to the main menu setting.

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

Downloaded from www.Manualslib.com manuals search engine

Adding a default gateway using the front control buttons and LCD

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

To add a default gateway to an interface

1. Press Enter to display the interface list.
2. Use the down arrow key to highlight the name of the interface connected to the Internet and press Enter.
3. Use the down arrow to highlight Default Gateway.
4. Press Enter and set the default gateway.
5. After you set the last digit of the default gateway, press Enter.
6. Press Esc to return to the main menu setting.

Verifying the front control buttons and LCD

To verify the interface settings entered from the front control buttons and LCD, go to the web-based manager, **System > Network > Interface**. The interface IP addresses entered from the front control buttons and LCD should be displayed.

Verify the connection

To verify your connection, try the following:

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

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

Using the command line interface

You can also configure the FortiGate unit using the command line interface (CLI). For information about connecting to the CLI, see "Connecting to the CLI" on page 23.

Configuring the FortiGate unit to operate in NAT/Route mode

Use the information you gathered in Table 13 on page 35 to complete the following procedures.

To add/change the administrator password

1. Log into the CLI.
2. Change the admin administrator password. Enter:

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


Downloaded from www.Manualslib.com manuals search engine

To configure interface

1 Log into the CLI.

2 Set the IP address and netmask of the internal interface to the internal IP address and netmask you recorded in Table 13 on page 35. Enter:

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

Example

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

3 Set the IP address and netmask of the external interface to the external IP address and netmask you recorded in Table 13 on page 35.

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

Example

```
config system interface
    edit wan1
       set mode static
       set ip 204.28.1.5 255.255.255.0
  end
```

To set the external interface to use DHCP, enter:

```
config system interface
    edit wan1
        set mode dhcp
  end
```

To set the external interface to use PPPoE, enter:

```
config system interface
    edit wan1
        set mode pppoe
        set connection enable
        set username <name_str>
        set password <psswrd>
  end
```

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

Downloaded from www.Manualslib.com manuals search engine

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 address. Enter:

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

Example

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

Adding a default route

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

To add a default route

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

```
config router static
    edit <seq_num>
        set dst <class_ip&net_netmask>
        set gateway <gateway_IP>
        set device <interface>
  end
```

Example

If the default gateway IP is 204.23.1.2 and this gateway is connected to WAN1:

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

Verify the connection

To verify the connection, try the following:

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

Downloaded from www.Manualslib.com manuals search engine

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

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

Connecting the FortiGate unit to the network(s)

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

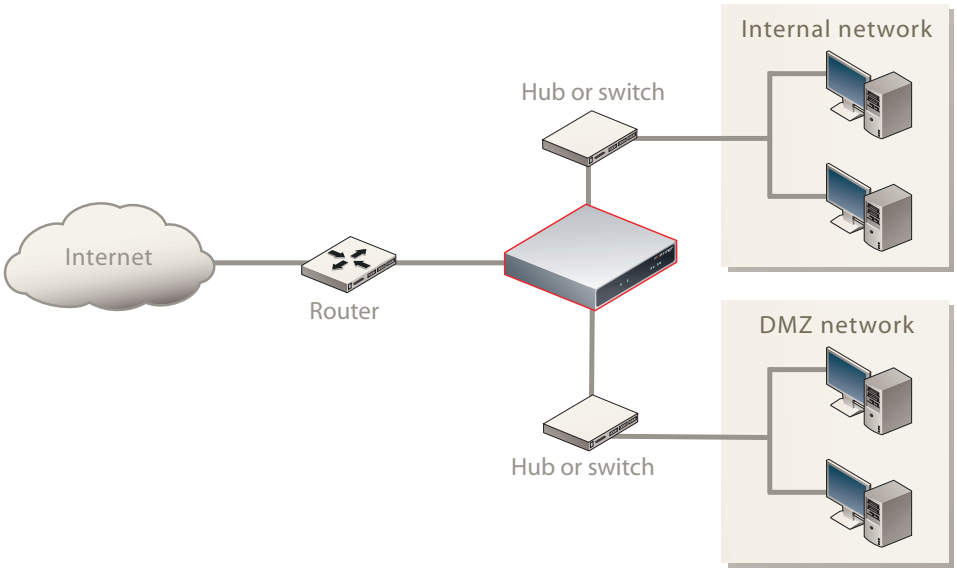
To connect the FortiGate unit

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

   Connect to the public switch or router provided by your ISP. If you are a DSL or cable subscriber, connect the External interface to the internal or LAN connection of your DSL or cable modem.
3. Optionally connect the DMZ interface to your DMZ network.

   You can use a DMZ network to provide access from the Internet to a web server or other server without installing the servers on your internal network.

Figure 11: NAT/Route mode connections.



Configuring the networks

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

- For the internal network, change the default gateway address of all computers and routers connected directly to your internal network to the IP address of the FortiGate internal interface.

Downloaded from www.Manualslib.com manuals search engine

- 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 external interface.

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

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

Transparent mode installation

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

- Preparing to configure Transparent mode
- Using the web-based manager
- Using the front control buttons and LCD
- Using the command line interface
- Connecting the FortiGate unit to your network

Preparing to configure Transparent mode

Use Table 15 on page 42 to gather the information you need to customize Transparent mode settings.

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

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

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

Table 15: 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:	_____ . _____ . _____ . _____ _____ . _____ . _____ . _____

Downloaded from www.Manualslib.com manuals search engine

Using the web-based manager

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 21. The first time you connect to the FortiGate unit, it is configured to run in NAT/Route mode.

To switch to Transparent mode using the web-based manager

1. Go to **System > Status**.
2. Select Change beside the Operation Mode.
3. Select Transparent in the Operation Mode list.
4. Type the Management IP/Netmask address and the Default Gateway address you gathered in Table 15 on page 42.
5. Select Apply.

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

To configure DNS server settings

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

Using the front control buttons and LCD

This procedure describes how to use the front control buttons and LCD to configure Transparent mode and Transparent mode IP addresses. Use the information you recorded in Table 15 on page 42 to complete this procedure.

To change the management IP address and netmask

1. Press Enter to display the option list.
2. Use the up or down arrows to highlight Management Interface.
3. Set the management interface IP address.

   Use the up and down arrow keys to increase or decrease the value of each IP address digit. Press Enter to move to the next digit. Press Esc to move to the previous digit.
4. After you set the last digit of the IP address, press Enter.
5. Use the down arrow to highlight Netmask.
6. Press Enter and set the management IP Netmask.
7. After you set the last digit of the Netmask, press Enter.
8. Press Esc to return to the main menu setting.

Downloaded from www.Manualslib.com manuals search engine

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

Adding a default gateway using the front control buttons and LCD

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

To add a default gateway to an interface

1. Press Enter to display the interface list.
2. Use the down arrow key to highlight the name of the interface connected to the Internet and press Enter.
3. Use the down arrow to highlight Default Gateway.
4. Press Enter and set the default gateway.
5. After you set the last digit of the default gateway, press Enter.
6. Press Esc to return to the main menu setting.

Verifying the front control buttons and LCD

To verify the interface settings entered from the front control buttons and LCD, go to the web-based manager, **System > Network > Interface**. The interface IP addresses entered from the front control buttons and LCD should be displayed.

Verify the connection

To verify your connection, try the following:

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

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

Using the command line interface

As an alternative to the web-based manager, you can begin the initial configuration of the FortiGate unit using the command line interface (CLI). To connect to the CLI, see "Connecting to the CLI" on page 23. Use the information you gathered in Table 15 on page 42 to complete the following procedures.

Downloaded from www.Manualslib.com manuals search engine

To change to Transparent mode using the CLI

1 Switch to Transparent mode. Enter:

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

After a few seconds, the following prompt appears:

```
Changing to TP mode
```

2 When the login prompt appears, enter the following:

```
get system settings
```

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

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

You should verify the DNS server settings are correct. The DNS settings carry over from NAT/Route mode and may not be correct for your specific Transparent mode configuration.

To verify the DNS server settings

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

```
show system dns
```

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

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

To configure DNS server settings

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

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

Reconnecting to the web-based manager

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

Downloaded from www.Manualslib.com manuals search engine

Connecting the FortiGate unit to your network

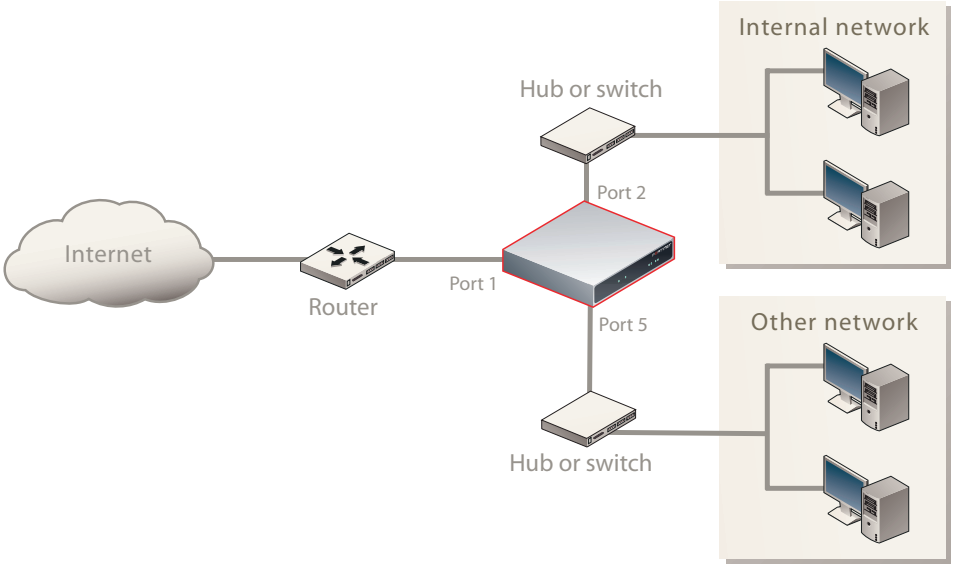
When you complete the initial configuration, you can connect the FortiGate unit between your internal network and the Internet.

To connect the FortiGate unit running in Transparent mode

1. Connect the Internal interface to the hub or switch connected to your internal network.
2. Connect the External interface to network segment connected to the external firewall or router.

   Connect to the public switch or router provided by your ISP.
3. Optionally connect the port or other interface that connects to other networks.

Figure 12: FortiGate-500A Transparent mode connections



Verify the connection

To verify the connection, try the following:

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

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

Next Steps

You can use the following information to configure FortiGate system time , to configure antivirus and attack definition updates. Refer to the *FortiGate Administration Guide* for complete information on configuring, monitoring, and maintaining your FortiGate unit.

Downloaded from www.Manualslib.com manuals search engine

Set the date and time

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

To set the date and time

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

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

To use NTP to set the FortiGate date and time

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

Updating antivirus and IPS signatures

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

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

You can update your antivirus and IPS signatures using the web-based manager or the CLI. Before you can begin receiving updates, you must register your FortiGate unit from the Fortinet web page.

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

Downloaded from www.Manualslib.com manuals search engine

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

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

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

Updating antivirus and IPS signatures from the web-based manager

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

To update antivirus definitions and IPS signatures

1. Go to **System > Maintenance > FortiGuard Center**.
2. Select the blue arrow for AntiVirus and IPS Downloads to expand the options.
3. Select Update Now to update the antivirus definitions.

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

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

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

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

Updating the IPS signatures from the CLI

You can also update IPS signatures using the CLI interface.

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

To update IPS signatures using the CLI

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

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


Downloaded from www.Manualslib.com manuals search engine

Scheduling antivirus and IPS updates

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

To enable schedule updates from the web-based manager

1. Go to **System > Maintenance > FortiGuard Center**.
2. Select the blue arrow for AntiVirus and IPS Downloads to expand the options.
3. Select the Scheduled Update check box.
4. Select one of the following to check for and download updates.

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

5. Select Apply.

The FortiGate unit starts the next scheduled update according to the new update schedule. Whenever the FortiGate unit runs a scheduled update, the event is recorded in the FortiGate event log.

To enable schedule updates from the CLI

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

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

Example

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

Adding an override server

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

To add an override server from the web-based manager

1. Go to **System > Maintenance > FortiGuard Center**.
2. Select the blue arrow for AntiVirus and IPS Downloads to expand the options.
3. Select the Use override server address check box.

Downloaded from www.Manualslib.com manuals search engine

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

5 Select Apply.

The FortiGate unit tests the connection to the override server.

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

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

To add an override server using the CLI

1 Log into the CLI.

2 Enter the following command:

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


Downloaded from www.Manualslib.com manuals search engine

FortiGate Firmware

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

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

This section includes the following topics:

- Upgrading to a new firmware version
- Reverting to a previous firmware version
- Installing firmware images from a system reboot using the CLII
- Testing a new firmware image before installing it
- Testing a new firmware image before installing it

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

Upgrading to a new firmware version

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

Upgrading the firmware using the web-based manager

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

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

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

To upgrade the firmware using the web-based manager

1. Copy the firmware image file to your management computer.
2. Log into the web-based manager as the admin administrative user.
3. Go to **System > Status**.
4. Under **System Information > Firmware Version**, select Update.
5. Type the path and filename of the firmware image file, or select Browse and locate the file.

Downloaded from www.Manualslib.com manuals search engine

6 Select OK.

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

7 Log into the web-based manager.

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

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

Upgrading the firmware using the CLI

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

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

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

To upgrade the firmware using the CLI

1 Make sure the TFTP server is running.

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

3 Log into the CLI.

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

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

```
execute ping 192.168.1.168
```

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

```
execute restore image <name_str> <tftp_ip4>
```

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

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

The FortiGate unit responds with the message:

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

6 Type `y`.

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

7 Reconnect to the CLI.

Downloaded from www.Manualslib.com manuals search engine

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

```
get system status
```

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

```
execute update-now
```

Reverting to a previous firmware version

Use the web-based manager or CLI procedure to revert to a previous firmware version. This procedure reverts the FortiGate unit to its factory default configuration.

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

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

Before beginning this procedure, it is recommended that you:

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

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

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

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

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

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

1 Copy the firmware image file to the management computer.

2 Log into the FortiGate web-based manager.

3 Go to **System > Status**.

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

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

6 Select OK.

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

7 Log into the web-based manager.

Downloaded from www.Manualslib.com manuals search engine

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

9 Restore your configuration.

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

10 Update antivirus and attack definitions.

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

Reverting to a previous firmware version using the CLI

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

Before beginning this procedure, it is recommended that you:

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

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

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

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

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

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

To revert to a previous firmware version using the CLI

1 Make sure the TFTP server is running

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

3 Log into the FortiGate CLI.

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

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

```
execute ping 192.168.1.168
```


Downloaded from www.Manualslib.com manuals search engine

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

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

Where `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `v280image.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image v2.80image.out 192.168.1.168
```

The FortiGate unit responds with this message:

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

6 Type `y`.

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

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

7 Type `y`.

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

8 Reconnect to the CLI.

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

```
get system status
```

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

```
execute restore config <name_str> <tftp_ip4>
```

11 Update antivirus and attack definitions.

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

```
execute update-now.
```


Downloaded from www.Manualslib.com manuals search engine

Installing firmware images from a system reboot using the CLI

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

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9 serial cable.

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

For this procedure you:

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

Before beginning this procedure, it is recommended that you:

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

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

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

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

To install firmware from a system reboot

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

```
execute ping 192.168.1.168
```


Downloaded from www.Manualslib.com manuals search engine

6 Enter the following command to restart the FortiGate unit.

```
execute reboot
```

The FortiGate unit responds with the following message:

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

7 Type `y`.

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

- FortiGate unit running v2.x BIOS

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

- FortiGate unit running v3.x BIOS

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

Immediately press any key to interrupt the system startup.

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

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

- FortiGate unit running v2.x BIOS

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

  Go to step 9.

- FortiGate unit running v3.x BIOS

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

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

The following message appears:

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

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

The following message appears:

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

10 Type an IP address the FortiGate unit can use to connect to the TFTP server. The IP address can be any IP address that is valid for the network the interface is connected to. Make sure you do not enter the IP address of another device on this network.

The following message appears:

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


Downloaded from www.Manualslib.com manuals search engine

11 Enter the firmware image filename and press Enter.

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

- FortiGate unit running v2.x BIOS

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

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

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

  or

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

12 Type `D`.

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

Restoring the previous configuration

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

```
config system interface
    edit internal
        set ip <address_ip4mask>
        set allowaccess {ping https ssh telnet http}
    end
```

After changing the interface address, you can access the FortiGate unit from the web-based manager and restore the configuration. For details, see the *FortiGate Administration Guide*.

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

The FortiUSB key

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

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

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

Downloaded from www.Manualslib.com manuals search engine

Backup and Restore from the FortiUSB key

Use the FortiUSB key to either backup a configuration file or restore a configuration file. You should always make sure the FortiUSB key is properly install before proceeding since the FortiGate unit must recognize that the key is installed in its USB port.

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

To backup configuration using the web-based manager

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

To restore configuration web-based manager

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

To backup configuration using the CLI

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

```
exec backup config usb <filename>
```

3. Enter the following command to check the configuration files are on the key:

```
exec usb-disk list
```

To restore configuration using the CLI

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

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

The FortiGate unit responds with the following message:

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

3. Type `y`.

Using the USB Auto-Install feature

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

Downloaded from www.Manualslib.com manuals search engine

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

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

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

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

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

To configure the USB Auto-Install using the CLI

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

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

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

```
get system status
```

Additional CLI Commands for the FortiUSB key

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

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

Downloaded from www.Manualslib.com manuals search engine

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

Testing a new firmware image before installing it

You can test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiGate unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure "Upgrading to a new firmware version" on page 51.

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

For this procedure you:

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

To test the new firmware image

1. Connect to the CLI using a RJ-45 to DB-9 serial cable and FortiGate console port.
2. Make sure the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Make sure the internal interface is connected to the same integer as the TFTP server.

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

   ```
   execute ping 192.168.1.168
   ```

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

   ```
   execute reboot
   ```

6. As the FortiGate unit reboots, press any key to interrupt the system startup. As the FortiGate unit starts, a series of system startup messages are displayed. When one of the following messages appears:
   - FortiGate unit running v2.x BIOS

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

   - FortiGate unit running v3.x BIOS

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

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

Downloaded from www.Manualslib.com manuals search engine

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

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

- FortiGate unit running v2.x BIOS

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

  Go to step 9.

- FortiGate unit running v3.x BIOS

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

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

The following message appears:

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

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

The following message appears:

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

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

The IP address must be on the same network as the TFTP server, but make sure you do not use the IP address of another device on the network.

The following message appears:

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

11 Enter the firmware image file name and press Enter.

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

- FortiGate unit running v2.x BIOS

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

  Type `n`.

- FortiGate unit running v3.x BIOS

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

  or

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

12 Type `R`.

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

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

Downloaded from www.Manualslib.com manuals search engine

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

```
get system status
```

You can test the new firmware image as required.

Downloaded from www.Manualslib.com manuals search engine

Downloaded from www.Manualslib.com manuals search engine

Index

A

adding a default route 36, 40
air flow 19
antivirus updates 47

C

certificate, security 22
CLI
  additional commands for FortiUSB key 60
  connecting to 23
  upgrading the firmware 52
comments, documentation 13
configuration
  DHCP 35
  PPPoE 35
connecting
  to the CLI 23
  to web-based manager 21
customer service 13

D

dashboard, system 23
default
  adding a route 36
default gateway
  using the LCD, front control buttons 38, 44
documentation
  commenting on 13
  Fortinet 11

F

factory default
  firewall configuration 29
  NAT/Route mode config 27
  protection profiles 29
firmware
  backup and restore from FortiUSB key 59
  installing from system reboot, CLI 56
  restoring previous configuration 58
  reverting to a previous version 53
  testing new firmware 61
  upgrading firmware version 51
  upgrading using CLI 52
  upgrading using web-based manager 51
FortiGate documentation
  commenting on 13
Fortinet customer service 13
Fortinet documentation 11
Fortinet Family Products 8
  FortiBridge 10
  FortiClient 9
  FortiGuard 8
  FortiLog 9
  FortiMail 9
  FortiManager 10
  FortiReporter 10
Fortinet Knowledge Center 12
FortiUSB key 61
  additional CLI commands 60
  backup and restore 59
  USB Auto-Install 59
front control buttons and LCD 24

I

introduction
  Fortinet documentation 11
IPS signature updates 47

L

LCD front control buttons 24

M

Mechanical loading 19

N

NAT/Route mode
  using LCD, front control buttons 37
  using the CLI 38
NTP server
  synchronize 47

P

ping requests, preventing public FortiGate interface from responding to 33
products, Fortinet family 8
protection profiles, default 29

R

reconnecting to web-based manager 45
registering FortiGate unit 8
restoring
  default settings 30
  previous firmware configuration 58
reverting
  previous firmware using the CLI 54
  to a previous version 53

S

security certificate 22
synchronize with NTP server 47
System dashboard 23

T

technical support 13
time zone 47
Transparent mode
  using LCD, front control buttons 43

Downloaded from www.Manualslib.com manuals search engine

using the CLI 44
using web-based manager 43

U

updating
adding override server 49
antivirus and IPS, web-based manager 48
IPS using CLI 48
scheduling updates 49
updating antivirus and IPS signatures 47
upgrading
firmware using the CLI 52
firmware using web-based manager 51
USB Auto-Install 59
using LCD, front control buttons 37, 43
using the web-based manager 43

V

verifying
connection 40
connection, LCD front control buttons 38, 44
connection, web-based manager 37
LCD, front control buttons 38, 44
web-based manager, config 37

W

web-based manager
connecting 21

Downloaded from www.Manualslib.com manuals search engine

www.fortinet.com

Downloaded from www.Manualslib.com manuals search engine

www.fortinet.com

Downloaded from www.Manualslib.com manuals search engine

Other ManualsLib Projects

www.manualslib.com

www.manualslib.de

www.manualslib.es

www.manualslib.fr

www.manualslib.nl

www.manualslib.mx

www.manualslib.tech 30+ Languages