



# FortiGate<sup>®</sup>

Version 4.0

Desktop Install Guide

## **FortiGate Desktop Install Guide**

Version 4.0

01 May 2009

01-400-95522-20090501

© Copyright 2009 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/Class B Part 15 CSA/CUS



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

# Contents

|  |           |
|--|-----------|
| <b>Introduction .....</b>                          | <b>3</b>  |
| <b>Registering your Fortinet product.....</b>      | <b>3</b>  |
| <b>Customer service and technical support.....</b> | <b>3</b>  |
| <b>Fortinet documentation .....</b>                | <b>4</b>  |
| Fortinet Tools and Documentation CD .....          | 4         |
| Fortinet Knowledge Center .....                    | 4         |
| Comments on Fortinet technical documentation ..... | 4         |
| <b>Conventions .....</b>                           | <b>4</b>  |
| IP addresses.....                                  | 4         |
| CLI constraints.....                               | 4         |
| Notes, Tips and Cautions .....                     | 4         |
| Typographical conventions .....                    | 5         |
| <b>Installing .....</b>                            | <b>7</b>  |
| <b>Environmental specifications .....</b>          | <b>7</b>  |
| <b>Cautions and warnings.....</b>                  | <b>8</b>  |
| Grounding.....                                     | 8         |
| Rack mount instructions .....                      | 8         |
| Mounting.....                                      | 8         |
| <b>Plugging in the FortiGate unit.....</b>         | <b>9</b>  |
| Connecting to the network .....                    | 9         |
| <b>Turning off the FortiGate unit .....</b>        | <b>9</b>  |
| <b>Configuring.....</b>                            | <b>11</b> |
| <b>NAT vs. transparent mode .....</b>              | <b>11</b> |
| NAT mode.....                                      | 11        |
| Transparent mode .....                             | 12        |
| <b>Connecting to the FortiGate unit .....</b>      | <b>12</b> |
| Connecting to the web-based manager.....           | 12        |
| Connecting to the CLI .....                        | 13        |
| <b>Configuring NAT mode .....</b>                  | <b>13</b> |
| Configure the interfaces.....                      | 14        |
| Configure a DNS server.....                        | 16        |
| Add a default route and gateway .....              | 17        |
| Add firewall policies .....                        | 18        |
| <b>Configuring transparent mode .....</b>          | <b>20</b> |
| Switching to transparent mode .....                | 20        |
| Configure a DNS server .....                       | 21        |

|   |           |
|---|-----------|
| Add firewall policies.....  | 21        |
| <b>Verifying the configuration .....</b>                            | <b>23</b> |
| <b>Backing up the configuration .....</b>                           | <b>23</b> |
| <b>Restoring a configuration .....</b>                              | <b>24</b> |
| <b>Additional configuration.....</b>                                | <b>25</b> |
| Setting the time and date.....                                      | 25        |
| Set the Administrator password.....                                 | 26        |
| Configuring FortiGuard .....  | 27        |
| Updating antivirus and IPS signatures .....                         | 27        |
| <b>Advanced configuration .....</b>                                 | <b>29</b> |
| <b>Protection profiles .....</b>                                    | <b>29</b> |
| <b>Firewall policies .....</b>                                      | <b>30</b> |
| Configuring firewall policies .....                                 | 31        |
| <b>Antivirus options.....</b>                                       | <b>31</b> |
| <b>AntiSpam options .....</b>                                       | <b>32</b> |
| <b>Web filtering .....</b>  | <b>33</b> |
| <b>Data leak prevention .....</b>                                   | <b>34</b> |
| <b>Application control .....</b>                                    | <b>34</b> |
| <b>Logging .....</b>  | <b>34</b> |
| <b>FortiGate Firmware .....</b>                                     | <b>35</b> |
| <b>Downloading firmware.....</b>                                    | <b>35</b> |
| <b>Using the web-based manager .....</b>                            | <b>36</b> |
| Upgrading the firmware .....  | 36        |
| Reverting to a previous version .....                               | 36        |
| Backup and Restore from a USB key .....                             | 37        |
| Using the USB Auto-Install .....                                    | 37        |
| <b>Using the CLI .....</b>  | <b>38</b> |
| Reverting to a previous version .....                               | 38        |
| <b>Installing firmware from a system reboot using the CLI .....</b> | <b>40</b> |
| Restoring the previous configuration .....                          | 41        |
| Backup and Restore from a USB key .....                             | 42        |
| Using the USB Auto-Install .....                                    | 42        |
| Additional CLI Commands for a USB key.....                          | 43        |
| <b>Testing new firmware before installing.....</b>                  | <b>43</b> |
| <b>Index.....</b>   | <b>1</b>  |

# Introduction

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

FortiGate® ASIC-accelerated multi-threat security systems improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network. FortiGate Systems are ICSA-certified for Antivirus, Firewall, IPSec, SSL-TLS, IPS, Intrusion detection, and AntiSpyware services.

FortiGate Systems are dedicated, easily managed security devices that deliver a full suite of capabilities including:

- Application-level services such as virus protection, intrusion protection, spam filtering, web content filtering, IM, P2P, and VoIP filtering
- Network-level services such as firewall, intrusion detection, IPSec and SSL VPN, and traffic shaping
- Management services such as user authentication, logging, reporting with FortiAnalyzer, administration profiles, secure web and CLI administrative access, and SNMP.

The FortiGate security system uses Fortinet's Dynamic Threat Prevention System (DTPS™) technology, which leverages breakthroughs in chip design, networking, security and content analysis. The unique ASIC-accelerated 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.

This chapter contains the following topics:

- [Registering your Fortinet product](#)
- [Customer service and technical support](#)
- [Fortinet documentation](#)
- [Conventions](#)

## Registering your Fortinet product

Before you begin, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Center article [Registration Frequently Asked Questions](#).

## Customer service and technical support

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

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Center article [What does Fortinet Technical Support require in order to best assist the customer?](#)

## Fortinet documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

### Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

### Fortinet Knowledge Center

The Fortinet Knowledge Center provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Center at <http://kc.fortinet.com>.

### Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## Conventions

Fortinet technical documentation uses the conventions described below.

### IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at <http://ietf.org/rfc/rfc1918.txt?number-1918>.

### CLI constraints

CLI constraints, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable input for a given parameter or variable value. CLI constraint conventions are described in the CLI Reference document for each product.

### Notes, Tips and Cautions

Fortinet technical documentation uses the following guidance and styles for notes, tips and cautions.



**Tip:** Highlights useful additional information, often tailored to your workplace activity.



**Note:** Also presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.



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

## Typographical conventions

Fortinet documentation uses the following typographical conventions:

**Table 1: Typographical conventions in Fortinet technical documentation**

| Convention   | Example  |
|--|--|
| <b>Button, menu, text box, field, or check box label</b> | From <i>Minimum log level</i> , select <i>Notification</i> .   |
| <b>CLI input</b>   | <pre>config system dns   set primary &lt;address_ipv4&gt; end</pre>  |
| <b>CLI output</b>  | <pre>FGT-602803030703 # get system settings comments           : (null) opmode             : nat</pre>   |
| <b>Emphasis</b>  | HTTP connections are <b><i>not</i></b> secure and can be intercepted by a third party.   |
| <b>File content</b>                                      | <pre>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt; &lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</pre> |
| <b>Hyperlink</b>   | Visit the Fortinet Technical Support web site, <a href="https://support.fortinet.com">https://support.fortinet.com</a> .   |
| <b>Keyboard entry</b>                                    | Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .   |
| <b>Navigation</b>  | Go to <code>VPN &gt; IPSEC &gt; Auto Key (IKE)</code> .  |
| <b>Publication</b>                                       | For details, see the <a href="#">FortiGate Administration Guide</a> .  |



# Installing

This chapter describes installing your Fortinet unit in your server room, environmental specifications and how to mount the Fortinet in a rack if applicable.

This chapter contains the following topics:

- [Environmental specifications](#)
- [Cautions and warnings](#)
- [Plugging in the FortiGate unit](#)
- [Plugging in the FortiGate unit](#)
- [Turning off the FortiGate unit](#)

## Environmental specifications

Before you begin, review the environmental specifications to ensure proper operation of the FortiGate unit.

- Operating temperature: 32 to 104°F (0 to 40°C)  
If you install the Fortinet unit in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, make sure to install the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.
- Storage temperature: -13 to 158°F (-25 to 70°C)
- Humidity: 5 to 90% non-condensing
- Air flow - For rack installation, make sure that the amount of air flow required for safe operation of the equipment is not compromised.
- For free-standing installation, make sure that the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

This device complies with part FCC Class A or Class B, Part 15, UL/CUL, C Tick, CE and VCCI. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

The equipment compliance with FCC radiation exposure limit set forth for uncontrolled Environment.

## Cautions and warnings

Review the following cautions before installing your Fortinet unit.



**Caution:** Risk of Explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions



**Caution:** To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

### Grounding

- Ensure the Fortinet unit is connected and properly grounded to a lightning and surge protector. WAN or LAN connections that enter the premises from outside the building should be connected to an Ethernet CAT5 (10/100 Mb/s) surge protector.
- Shielded Twisted Pair (STP) Ethernet cables should be used whenever possible rather than Unshielded Twisted Pair (UTP).
- Do not connect or disconnect cables during lightning activity to avoid damage to the Fortinet unit or personal injury.

### Rack mount instructions

**Elevated operating ambient** - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T<sub>ma</sub>) specified by the manufacturer.

**Reduced air flow** - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

**Mechanical loading** - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

**Circuit overloading** - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

**Reliable earthing** - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

### Mounting

If required to fit into a rack unit, remove the rubber feet from the bottom of the Fortinet unit. Place the FortiGate unit on any flat, stable surface. Ensure the unit has sufficient clearance on each side to ensure adequate airflow for cooling.

## Plugging in the Fortinet unit

Use the following steps to connect the power supply to the FortiGate unit.

### To power on the FortiGate unit

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

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

### Connecting to the network

Using the supplied Ethernet cable, connect one end of the cable to your router or modem, whatever the connection is to the Internet. Connect the other end to the Fortinet unit. Connect to either the External, WAN port, or port 1. Connect additional cable to the Internal port or port 2 and your internal hub or switch.

## Turning off the Fortinet unit

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

### To power off the Fortinet 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 Disconnect the power cables from the power supply.



# Configuring

This section provides an overview of the operating modes of the Fortinet unit, NAT/Route and transparent, and how to configure the unit for each mode. There are two ways you can configure the unit, through either the web-based manager or the command line interface (CLI). This section will step through both methods. Use whichever you are most comfortable with.

This section includes the following topics:

- [NAT vs. transparent mode](#)
- [Connecting to the FortiGate unit](#)
- [Verifying the configuration](#)
- [Backing up the configuration](#)
- [Restoring a configuration](#)
- [Additional configuration](#)

## NAT vs. transparent mode

The Fortinet unit can run in two different modes, depending on your network infrastructure and requirements. You can choose between NAT/Route mode and transparent mode. Both include the same robust network security features such as antispam, antivirus, VPN and firewall policies.

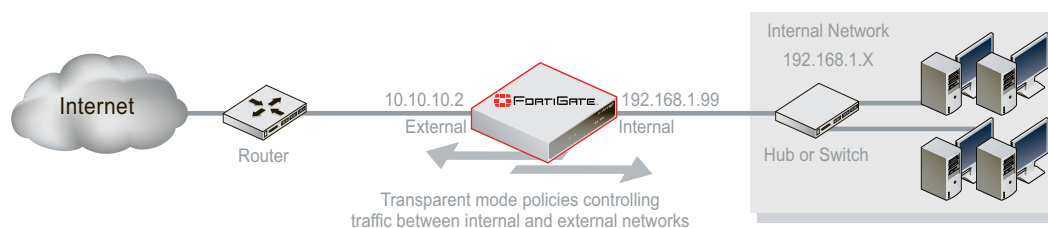
### NAT mode

In NAT/Route mode, the Fortinet unit is visible to the network. Like a router, all its interfaces are on different subnets.

In NAT mode, each port is on a different subnet, enabling you to have a single IP address available to the public Internet. The Fortinet unit performs network address translation before sending the packet to the destination network or receiving a packet from the destination network.

In Route mode, there is no address translation.

**Figure 1: Fortinet unit in NAT mode**



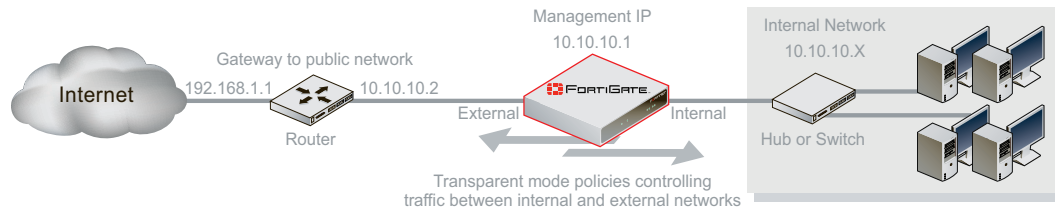
You typically use NAT/Route mode when the Fortinet unit is operating as a gateway between private and public networks. In this configuration, you would create NAT mode firewall policies to control traffic flowing between the internal, private network and the external, public network, usually the Internet.

In this guide, unless otherwise stated, references to NAT mode apply to both NAT and Route mode.

## Transparent mode

In transparent mode, the Fortinet 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 to make configuration changes. The management IP address is also used for antivirus and attack definition updates.

**Figure 2: Fortinet unit in transparent mode**



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

## Connecting to the Fortinet unit

To configure, maintain and administer the Fortinet unit, you need to connect to it. There are two methods for these tasks:

- using the web-based manager: a GUI interface that you connect to using a current web browser such as FireFox or Internet Explorer.
- using the command line interface (CLI): a command line interface similar to DOS or UNIX commands that you connect to using an SSH terminal or Telnet terminal.

### Connecting to the web-based manager

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 a common web browser
- an Ethernet cable.

#### To connect to the web-based manager

- 1 Set the IP address of the management computer to the static IP address 192.168.1.2 with a netmask of 255.255.255.0.
- 2 Using the Ethernet cable, connect the internal interface of the Fortinet unit to the computer Ethernet connection.
- 3 Start your browser and enter the address `https://192.168.1.99`. (remember to include the “s” in `https://`).

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

The first warning prompts you to accept and optionally install the Fortinet unit's self-signed security certificate. If you do not accept the certificate, the Fortinet 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 Fortinet 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 Fortinet unit redirects the connection. This is an informational message. Select OK to continue logging in.

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

## Connecting to the CLI

To connect to the FortiGate CLI you require:

- a computer with an available communications port
- a serial cable, either an RJ-45 to DB-9 or null modem cable, whichever was included in your FortiGate package
- terminal emulation software such as HyperTerminal for Microsoft Windows.



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

### To connect to the CLI

- 1 Connect the 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 then select OK:

|                        |      |
|------------------------|------|
| <b>Bits per second</b> | 9600 |
| <b>Data bits</b>       | 8    |
| <b>Parity</b>          | None |
| <b>Stop bits</b>       | 1    |
| <b>Flow control</b>    | None |

- 5 Press Enter to connect to the FortiGate CLI.
- 6 When the login prompt appears, type `admin` and press Enter twice.  
Type `?` to list available commands. For information about how to use the CLI, see the [FortiGate CLI Reference](#).

## Configuring NAT mode

When configuring NAT mode, you need to define interface addresses and default routes, and simple firewall policies. You can use the web-based manager or the CLI to configure the Fortinet unit in NAT/Route mode.

## Configure the interfaces

When shipped, the Fortinet unit has a default address of 192.168.1.99 and a netmask of 255.255.255.0. for either the Port 1 or Internal interface. You need to configure this and other ports for use on your network.



**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 interface for manual addressing - web-based manager

- 1 Go to *System > Network > Interface*.
- 2 Select the *Edit* icon for an interface.
- 3 Enter the *IP address* and *netmask* for the interface.

### To configure an interface for manual addressing - CLI

```
config system interface
    edit <interface_name>
        set mode static
        set ip <interface_ipv4mask>
    end
```

### To configure DHCP addressing - web-based manager

- 1 Go to *System > Network > Interface*.
- 2 Select the *Edit* icon for an interface.
- 3 Select *DHCP* and complete the following:

|   |   |
|---|---|
| <b>Distance</b>                             | Enter the administrative distance, between 1 and 255 for the default gateway retrieved from the DHCP server. The administrative distance specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. |
| <b>Retrieve default gateway from server</b> | Enable to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table.   |
| <b>Override internal DNS</b>                | Enable to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page on <i>System &gt; Network &gt; Options</i> . You should also enable Obtain DNS server address automatically in <i>System &gt; Network &gt; Options</i> .                                |

- 4 Select *OK*.

Figure 3: Configuring DHCP addressing

**Addressing mode**

Manual  DHCP  PPPoE

Distance:

Retrieve default gateway from server.

Override internal DNS.

**To configure DHCP addressing - CLI**

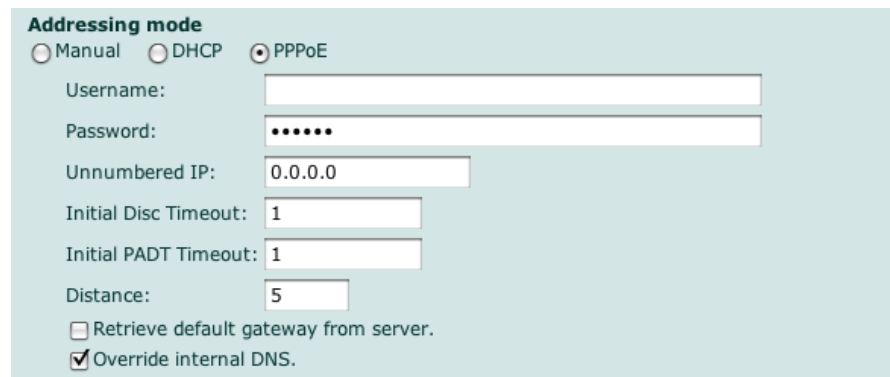
```
config system interface
  edit external
    set mode dhcp
    set distance <integer>
    set defaultgw enable
  end
```

**To configure DHCP addressing - web-based manager**

- 1 Go to *System > Network > Interface*.
- 2 Select the *Edit* icon for an interface.
- 3 Select *PPPoE*, and complete the following:

|   |   |
|---|---|
| <b>Username</b>                             | Enter the username for the PPPoE server. This may have been provided by your Internet Service Provider.   |
| <b>Password</b>                             | Enter the password for the PPPoE server for the above user name.  |
| <b>Unnumbered IP</b>                        | Specify the IP address for the interface. If your Internet Service Provider has assigned you a block of IP addresses, use one of these IP addresses. Alternatively, you can use, or borrow, the IP address of a configured interface on the router. You may need to do this to minimize the number of unique IP addresses within your network.<br>If you are borrowing an IP address, remember the interface must be enabled, and Ethernet connected. |
| <b>Initial Disc Timeout</b>                 | Initial discovery timeout in seconds. The amount of time to wait before starting to retry a PPPoE discovery. To disable the discovery timeout, set the value to 0.  |
| <b>Initial PADT Timeout</b>                 | Initial PPPoE Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE session if it is idle for this number of seconds. Your Internet Service Provider must support PADT. To disable the PADT timeout, set the value to 0.  |
| <b>Distance</b>                             | Enter the administrative distance, between 1 and 255, for the default gateway retrieved from the DHCP server. The administrative distance specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route.  |
| <b>Retrieve default gateway from server</b> | Enable to retrieve a default gateway IP address from the DHCP server. The default gateway is added to the static routing table.   |
| <b>Override internal DNS</b>                | Enable to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page on <i>System &gt; Network &gt; Options</i> . On Fortinet-100 units and lower, you should also enable Obtain DNS server address automatically in <i>System &gt; Network &gt; Options</i> .   |

- 4 Select *OK*.

**Figure 4: Configuring PPPoE addressing**


**Addressing mode**

Manual
  DHCP
  PPPoE

Username:

Password:

Unnumbered IP:

Initial Disc Timeout:

Initial PADT Timeout:

Distance:

Retrieve default gateway from server.  
 Override internal DNS.

**To configure PPPoE addressing - CLI**

```

config system interface
  edit external
    set mode pppoe
    set username <pppoe_username>
    set password <pppoe_password>
    set ipunnumbered <unnumbered_ipv4>
    set disc-retry-timeout <pppoe_retry>
    set padt-retry-timeout <pppoe_retry>
    set distance <integer>
    set defaultgw enable
  end

```

**Configure a DNS server**

A DNS server is a service that converts symbolic node names to IP addresses. A domain name server (DNS server) implements the protocol. In simple terms, it acts as a phone book for the Internet. A DNS server matches domain names with the computer IP address. This enables you to use readable locations, such as fortinet.com when browsing the Internet.

DNS server IP addresses are typically provided by your Internet Service Provider.

**To configure DNS server settings - web-based manager**

- 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*.

**Figure 5: Configure a DNS server**

The screenshot shows the 'Networking Options' configuration page. Under the 'DNS Settings' section, the 'Primary DNS Server' is set to 192.168.110.9, the 'Secondary DNS Server' is set to 1.1.1.1, and the 'Local Domain Name' field is empty. Under the 'Dead Gateway Detection' section, the 'Detection Interval' is set to 5 seconds and the 'Fail-over Detection' is set to 5 lost consecutive pings. An 'Apply' button is located at the bottom of the configuration area.

**To configure DNS server settings - CLI**

```
config system dns
    set primary <dns_ipv4>
    set secondary <dns_ipv4>
end
```

**Add a default route and gateway**

A route provides the Fortinet unit with the information it needs to forward a packet to a particular destination. A static route causes packets to be forwarded to a destination other than the default gateway. You define static routes manually. Static routes control traffic exiting the Fortinet unit. You can specify through which interface the packet will leave and to which device the packet should be routed.

In the factory default configuration, entry number 1 in the Static Route list is associated with a destination address of 0.0.0.0/0.0.0.0, which means any/all destinations. This route is called the “static default route”. If no other routes are present in the routing table and a packet needs to be forwarded beyond the Fortinet unit, the factory configured static default route causes the Fortinet unit to forward the packet to the default gateway.

For an initial configuration, you must edit the factory configured static default route to specify a different default gateway for the Fortinet unit. This will enable the flow of data through the unit.

For details on adding additional static routes, see the [FortiGate Administration Guide](#).

**To modify the default gateway - web-based manager**

- 1 Go to *Router > Static*.
- 2 Select the *Edit* icon for the default route
- 3 In the *Gateway* field, type the IP address of the next-hop router where outbound traffic is directed.
- 4 If the Fortinet unit reaches the next-hop router through a different interface (compared to the interface that is currently selected in the *Device* field), select the name of the interface from the *Device* field.
- 5 Select *OK*.

**Figure 6: Configure the default gateway**
**To modify the default gateway - CLI**

```

config router static
    edit <sequence_num>
        set gateway <gateway_address_ipv4>
        set device <interface_name>
    end

```

**Add firewall policies**

Firewall policies enable traffic to flow through the Fortinet interfaces. Firewall policies define how the Fortinet unit processes the packets in a communication session. You can configure the firewall policies to allow only specific traffic, users and specific times when traffic is allowed.

For the initial installation, a single firewall policy that enables all traffic to flow through will enable you to verify your configuration is working. On lower-end units such a default firewall policy is already in place. For the high-end Fortinet units, you need to add a firewall policy.

The following steps add two policies that allows all traffic through the Fortinet unit, to enable you to continue testing the configuration on the network.

**To add an outgoing traffic firewall policy - web-based manager**

- 1 Go to *Firewall > Policy*.
- 2 Select *Create New*.
- 3 Set the following and select *OK*.

|                                   |  |
|-----------------------------------|--|
| <b>Source Interface/Zone</b>      | Select the port connected to the network.  |
| <b>Source Address</b>             | All  |
| <b>Destination Interface/Zone</b> | Select the port connected to the Internet. |
| <b>Destination Address</b>        | All  |
| <b>Schedule</b>                   | always                                     |
| <b>Service</b>                    | Any  |
| <b>Action</b>                     | Accept                                     |

**Figure 7: Creating an outgoing firewall policy**

|                            |          |          |
|----------------------------|----------|----------|
| Source Interface/Zone      | internal |          |
| Source Address             | all      | Multiple |
| Destination Interface/Zone | wan1     |          |
| Destination Address        | all      | Multiple |
| Schedule                   | always   |          |
| Service                    | ANY      | Multiple |
| Action                     | ACCEPT   |          |

**To add an outgoing traffic firewall policy - CLI**

```

config firewall policy
  edit <index_int>
    set srcintf <name_str>
    set srcaddr <name_str>
    set dstintf <name_str>
    set dstaddr <name_str>
    set schedule always
    set service ANY
    set action accept
  end
    
```

**To add an incoming traffic firewall policy - web-based manager**

- 1 Go to *Firewall > Policy*.
- 2 Select *Create New*.
- 3 Set the following and select *OK*.

- Source Interface**      Select the port connected to the Internet.
- Source Address**      All
- Destination Interface**      Select the port connected to the network.
- Destination Address**      All
- Schedule**              always
- Service**                Any
- Action**                 Accept

**Figure 8: Creating an incoming firewall policy**

|                            |          |          |
|----------------------------|----------|----------|
| Source Interface/Zone      | wan1     |          |
| Source Address             | all      | Multiple |
| Destination Interface/Zone | internal |          |
| Destination Address        | all      | Multiple |
| Schedule                   | always   |          |
| Service                    | ANY      | Multiple |
| Action                     | ACCEPT   |          |

**To add an incoming traffic firewall policy - CLI**

```

config firewall policy
  edit <index_int>
    set srcintf <name_str>
    set srcaddr <name_str>
    set dstintf <name_str>
    set dstaddr <name_str>
    set schedule always
    set service ANY
    set action accept
  end

```

To create an incoming traffic firewall policy, you use the same commands with the addresses reversed.

Firewall policy configuration is the same in NAT/Route mode and transparent mode.

These policies allow all traffic through. No protection profiles have been applied. Ensure you create additional firewall policies to accommodate your network requirements.

For details, see the [FortiGate Administration Guide](#).

## Configuring transparent mode

When configuring transparent mode, you need to switch to transparent mode and configure the management IP address, default routes, and simple firewall policies. You can use the web-based manager or the CLI to configure the Fortinet unit in transparent mode.

### Switching to transparent mode

The Fortinet unit comes preset to NAT mode. You need to switch to transparent mode.

**To switch to transparent mode - web-based manager**

- 1 Go to *System > Status*.
- 2 Under *System Information*, select *Change* beside the *Operation Mode*.
- 3 Select *Transparent*.
- 4 Enter the *Management IP/Netmask* address and the *Default Gateway* address.  
The default gateway IP address is required to tell the Fortinet unit where to send network traffic to other networks.
- 5 Select *Apply*.

**Figure 9: Switching to transparent mode**

| Mode                  |                 |
|-----------------------|-----------------|
| Operation Mode        | Transparent     |
| Management IP/Netmask | 0.0.0.0/0.0.0.0 |
| Default Gateway       | 0.0.0.0         |
| <b>Apply</b>          |                 |

### To switch to transparent mode

```
config system settings
    set opmode transparent
    set manageip <manage_ipv4>
    set gateway <gw_ipv4>
end
```

### Configure a DNS server

A DNS server is a service that converts symbolic node names to IP addresses. A domain name server (DNS server) implements the protocol. In simple terms, it acts as a phone book for the Internet. A DNS server matches domain names with the computer IP address. This enables you to use readable locations, such as fortinet.com when browsing the Internet.

DNS server IP addresses are typically provided by your Internet Service Provider.

#### To configure DNS server settings - web-based manager

- 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*.

Figure 10: Configure a DNS server

| Networking Options            |                            |
|-------------------------------|----------------------------|
| <b>DNS Settings</b>           |                            |
| Primary DNS Server            | 192.168.110.9              |
| Secondary DNS Server          | 1.1.1.1                    |
| Local Domain Name             |                            |
| <b>Dead Gateway Detection</b> |                            |
| Detection Interval            | 5 (seconds)                |
| Fail-over Detection           | 5 (lost consecutive pings) |
| <b>Apply</b>                  |                            |

#### To configure DNS server settings - CLI

```
config system dns
    set primary <dns_ipv4>
    set secondary <dns_ipv4>
end
```

### Add firewall policies

Firewall policies enable traffic to flow through the Fortinet interfaces. Firewall policies define the Fortinet unit process the packets in a communication session. You can configure the firewall policies to allow only specific traffic, users and specific times when traffic is allowed.

For the initial installation, a single firewall policy that enables all traffic through will enable you to verify your configuration is working. On lower-end units such a default firewall policy is already in place. For the higher end Fortinet units, you will need to add a firewall policy.

The following steps add two policies that allows all traffic through the Fortinet unit, to enable you to continue testing the configuration on the network.

### To add an outgoing traffic firewall policy - web-based manager

- 1 Go to *Firewall > Policy*.
- 2 Select *Create New*.
- 3 Set the following and select *OK*.

|                                   |  |
|-----------------------------------|--|
| <b>Source Interface/Zone</b>      | Select the port connected to the network.  |
| <b>Source Address</b>             | All  |
| <b>Destination Interface/Zone</b> | Select the port connected to the Internet. |
| <b>Destination Address</b>        | All  |
| <b>Schedule</b>                   | always                                     |
| <b>Service</b>                    | Any  |
| <b>Action</b>                     | Accept                                     |

Figure 11: Creating an outgoing firewall policy

|                            |          |          |
|----------------------------|----------|----------|
| Source Interface/Zone      | internal |          |
| Source Address             | all      | Multiple |
| Destination Interface/Zone | wan1     |          |
| Destination Address        | all      | Multiple |
| Schedule                   | always   |          |
| Service                    | ANY      | Multiple |
| Action                     | ACCEPT   |          |

### To add an outgoing traffic firewall policy - CLI

```
config firewall policy
  edit <index_int>
    set srcintf <name_str>
    set srcaddr <name_str>
    set dstintf <name_str>
    set dstaddr <name_str>
    set schedule always
    set service ANY
    set action accept
  end
```

### To add an incoming traffic firewall policy - web-based manager

- 1 Go to *Firewall > Policy*.
- 2 Select *Create New*.
- 3 Set the following and select *OK*.

|                              |  |
|------------------------------|--|
| <b>Source Interface</b>      | Select the port connected to the Internet. |
| <b>Source Address</b>        | All  |
| <b>Destination Interface</b> | Select the port connected to the network.  |
| <b>Destination Address</b>   | All  |

|                 |        |
|-----------------|--------|
| <b>Schedule</b> | always |
| <b>Service</b>  | Any    |
| <b>Action</b>   | Accept |

**Figure 12: Creating an incoming firewall policy**

|                            |          |          |
|----------------------------|----------|----------|
| Source Interface/Zone      | wan1     |          |
| Source Address             | all      | Multiple |
| Destination Interface/Zone | internal |          |
| Destination Address        | all      | Multiple |
| Schedule                   | always   |          |
| Service                    | ANY      | Multiple |
| Action                     | ACCEPT   |          |

### To add an incoming traffic firewall policy - CLI

```
config firewall policy
  edit <index_int>
    set srcintf <name_str>
    set srcaddr <name_str>
    set dstintf <name_str>
    set dstaddr <name_str>
    set schedule always
    set service ANY
    set action accept
  end
```

To create an incoming traffic firewall policy, you use the same commands with the addresses reversed.

Firewall policy configuration is the same in NAT/Route mode and transparent mode.

These policies allow all traffic through. No protection profiles have been applied. Ensure you create additional firewall policies to accommodate your network requirements.

## Verifying the configuration

Your Fortinet unit is now configured and connected to the network. To verify that the Fortinet unit is connected and configured correctly, use your web browser to browse a web site, or use your email client to send and receive email.

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.

Remember to verify the firewall policies. The firewall policies control the flow of information through the Fortinet unit. If the policies are not set up correctly, or are too restrictive, they can prohibit network traffic.

## Backing up the configuration

Once you have determined your Fortinet unit is configured and working correctly, it is extremely important that you back up your configuration. By backing up the configuration, you ensure that if you need to reset the unit for whatever reason, you will be able to quickly return it to operation with minimal effort.

**To back up the Fortinet configuration - web-based manager**

- 1 Go to *System > Maintenance > Backup & Restore*.
- 2 Select to back up to your *Local PC* or to a *USB key*.  
The *USB Disk* option will be grayed out if the Fortinet unit supports USB disks but none are connected.
- 3 Select *Encrypt configuration file*.  
Encryption must be enabled on the backup file to back up VPN certificates.
- 4 Enter a password and enter it again to confirm it. You will need this password to restore the file.
- 5 Select *Backup*.
- 6 The web browser will prompt you for a location to save the configuration file. The configuration file will have a *.conf* extension.

**Figure 13: Backing up the FortiGate configuration**
**To back up the FortiGate configuration - CLI**

```
execute backup configmanagement-station <comment>
```

or

```
execute backup configusb <backup_filename> [<backup_password>]
```

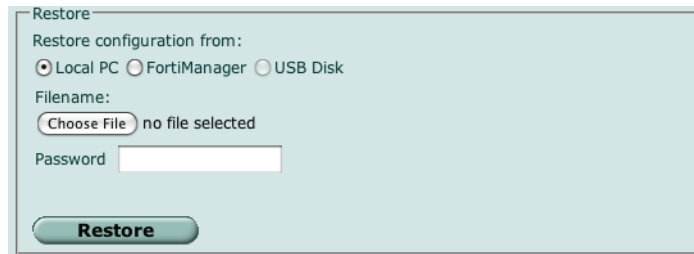
It is a good practice to backup the Fortinet configuration after any modification to any of the Fortinet settings. Alternatively, before performing an upgrade to the firmware, ensure you back up the configuration before upgrading. Should anything happen during the upgrade that changes the configuration, you can easily restore the saved configuration.

## Restoring a configuration

Should you need to restore a configuration file, use the following steps.

**To restore the Fortinet configuration - web-based manager**

- 1 Go to *System > Maintenance > Backup & Restore*.
- 2 Select to upload the configuration file to be restored from your *Local PC* or a *USB key*.  
The *USB Disk* option will be grayed out if the Fortinet unit supports USB disks but none are connected.
- 3 Enter the path and file name of the configuration file, or select *Browse* to locate the file.
- 4 Enter a password if required.
- 5 Select *Restore*.

**Figure 14: Restoring a FortiGate configuration****To back up the FortiGate configuration - CLI**

```
execute restore configmanagement-station normal 0  
or
```

```
execute restore configusb <filename> [<password>]
```

The Fortinet unit will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored. For information on verifying the configuration, see [“Verifying the configuration” on page 23](#).

## Additional configuration

Once the FortiGate unit is connected and traffic can pass through, several more configuration options are available. While not mandatory, they will help to ensure better control with the firewall.

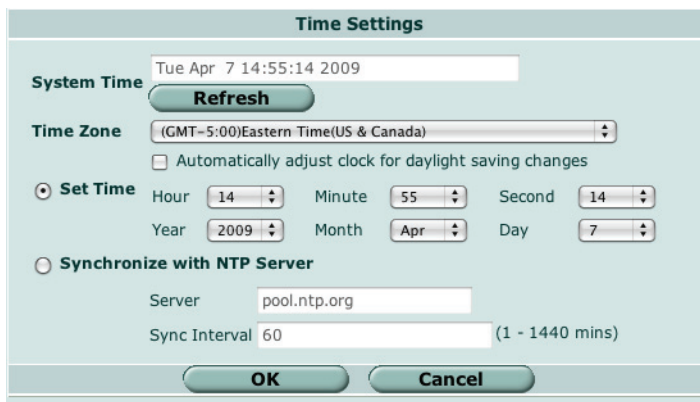
### Setting the time and date

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 Fortinet unit to automatically keep its time correct by synchronizing with a Network Time Protocol (NTP) server.

**To set the date and time - web-based manager**

- 1 Go to *System > Status*.
- 2 Under *System Information > System Time*, select *Change*.
- 3 Select your Time Zone.
- 4 Optionally, select *Automatically adjust clock for daylight saving changes*.
- 5 Select *Set Time* and set the FortiGate system date and time.
- 6 If you want to synchronize the time with an NTP server, enable the option.
- 7 Select *OK*.

Figure 15: Setting the time and date



**Set the time and date - CLI**

```
execute date [<date_str>]
execute time [<time_str>]
```



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

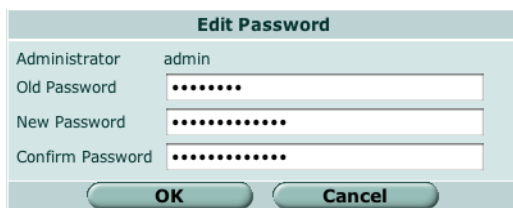
**Set the Administrator password**

The Fortinet unit ships with a default empty password. You will want to apply a password to prevent anybody logging into the Fortinet unit and changing configuration options.

**To change the administrator password - web-based manager**

- 1 Go to *System > Admin > Administrators*.
- 2 Select the *Change Password* icon and enter a new password.
- 3 Select *OK*.

Figure 16: Changing the Admin password



Alternatively, you can also add new administrator users by selecting *Create New*, however, you cannot remove the admin administrator. Applying a password for this account is recommended.

**Set the admin password - CLI**

```
config system admin
  edit admin
    set password <admin_password>
```

## Configuring FortiGuard

You need to configure the Fortinet unit to connect to the FortiGuard Distribution Network (FDN) to update the antivirus, antispam and IPS attack definitions.

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

Before you can begin receiving updates, you must register your Fortinet unit from the Fortinet web page. For more information, see [“Register your FortiGate unit”](#) on page 13.

## Updating antivirus and IPS signatures

After you have registered your Fortinet unit, you can update antivirus and IPS signatures. 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*.
- 2 Select the expand arrow for *AntiVirus and IPS Options* 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 System FortiGuard Center page lists new version information for antivirus definitions. The System Status page also displays new dates and version numbers for the antivirus definitions. Messages are recorded to the event log indicating whether or not the update was successful or not.



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

For more information on FortiGuard configuration, see the [FortiGate Administration Guide](#).



# Advanced configuration

The Fortinet unit and the FortiOS operating system provide a wide range of advanced features that enable you to control network and internet traffic and protect your network. This chapter describes some of these options and where to configure them, after you have completed basic configuration.

This chapter includes

- [Protection profiles](#)
- [Firewall policies](#)
- [Antivirus options](#)
- [AntiSpam options](#)
- [Web filtering](#)
- [Logging](#)

## Protection profiles

A protection profile is a group of settings you can adjust to suit your needs for network protection. Since protection profiles apply different protection settings to traffic controlled by firewall policies, you can tailor the settings to the type of traffic each policy handles.

Use protection profiles to configure:

- protocol recognition
- antivirus protection
- web filtering
- web category filtering
- application control
- data leak prevention
- spam filtering
- content archiving
- instant messaging filtering and access control
- P2P access and bandwidth control
- logging options for policies and configurations within the policies
- rate limiting for VoIP protocols.

Using protection profiles, you can customize types and levels of protection for different firewall policies.

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

The Fortinet unit is pre configured with four default protection profiles. In many cases you can use these default protection profiles, use them just as they are or as a starting point to create your own.

**Table 2: Default protection profiles**

|                   |   |
|-------------------|---|
| <b>Strict</b>     | Applies maximum protection to HTTP, FTP, IMAP, POP3, and SMTP traffic. The strict protection profile may not be useful under normal circumstances but it is available when maximum protection is required.  |
| <b>Scan</b>       | Applies virus scanning to HTTP, FTP, IMAP, POP3, and SMTP traffic.  |
| <b>Web</b>        | Applies virus scanning and web content blocking to HTTP traffic.  |
| <b>Unfiltered</b> | Applies no scanning, blocking or IPS. Use the unfiltered content profile if no content protection for content traffic is required. Add this protection profile to firewall policies for connections between highly trusted or highly secure networks where content does not need to be protected. |

The best way to begin creating your own protection profile is to open a predefined profile. This way you can see how a profile is set up, and then modify it to suit your requirements. You access protection profile options by going to *Firewall > Protection Profile*, and selecting Edit for one of the predefined profiles.

Protection profiles are used by the firewall policies to determine how network and Internet traffic is controlled, scanned and, when necessary, rejected. The protection profiles can be considered the rules of the firewall policy. Because of this, you should take some time to review the various options to consider what you want the firewall policies to do. If, after setting the protection profile and firewall policies, traffic is not flowing or flowing too much, verify your profile settings.

The number of options and configuration settings for the protection profile is too vast for this document. For details on each protection profile feature and setting, see the [FortiGate Administration Guide](#) or the [Fortinet Online Help](#).

## Firewall policies

Firewall policies are the instructions the Fortinet unit uses to decide what to do with a connection request. When the firewall receives a connection request, it analyzes it to extract its source address, destination address, and port number.

For the connection through the Fortinet unit to be successful, the source address, destination address, and service of the connection must match a firewall policy. The policy directs the firewall action for the connection. The action can be to allow the connection, deny the connection, require authentication before the connection is allowed, or process the packet as an IPSec VPN connection.

You can configure each firewall policy to route connections or apply network address translation (NAT) to translate source and destination IP addresses and ports. You also add protection profiles to firewall policies to apply different protection settings for the traffic controlled by firewall policies.

The Fortinet unit matches firewall policies by searching from the top of the firewall policy list and moving down until it finds the first match it, then implements the required address translation, blocking and other rules defined by the protection profile, and then passes on the packet information. This list order is important, because once the Fortinet unit finds a match to a policy, it will not continue down the list. You need to arrange policies in the policy list from more specific to more general.

For example, you may have two policies, one that blocks specific URLs or IP addresses, and another general policy that lets traffic through. If you put the general policy at the top, the Fortinet unit will act on the general policy, having calculated that the policy has been matched, and then stop. The second policy will be ignored and the Fortinet unit will let the URLs or IPs you wanted blocked get through.



**Note:** On the FortiGate-110C and lower, default firewall policies are in place to enable the flow of traffic right out of the box.

## Configuring firewall policies

To add or edit a firewall policy go to *Firewall > Policy* and select *Edit* on an existing policy, or select *Create New* to add a policy.

The *Source Interface/Zone* and *Destination Interface/Zone* match the firewall policy with the source and destination of a communication session. The *Address Name* matches the source and destination address of the communication session.

*Schedule* defines when the firewall policy is enabled. While most policies are always on, you can configure a firewall policy so that it is only on at specific times of the day. For example, you may want to block news and entertainment sites most of the day, except during lunch or after work, enabling your employees to view those sites only during non-working times.

*Service* matches the firewall policy with the service used by a communication session. This enables you to configure a policy for general web surfing and a different policy specifically for other traffic such as SMTP mail or FTP uploads and downloads.

*Action* defines how the Fortinet unit processes traffic. Specify an action to accept or deny traffic or configure a firewall encryption policy.

- Add *ACCEPT* policies that accept communication sessions. Using an accept policy, you can apply Fortinet features such as virus scanning and authentication to the communication session accepted by the policy.
- Add *DENY* policies to deny communication sessions.
- Add *IPSec* encryption policies to enable IPSec tunnel mode VPN traffic and *SSL VPN* encryption policies to enable SSL VPN traffic. Firewall encryption policies determine which types of IP traffic will be permitted during an IPSec or SSL VPN session.

Select *Protection Profile* to include apply a protection profile to the firewall policy for scanning of traffic passing through the Fortinet unit.

For details on the firewall policies features and settings, see the [FortiGate Administration Guide](#) or the [Fortinet Online Help](#).

## Antivirus options

The Fortinet unit's antivirus configuration prevents malicious files from entering and infecting your network environment.

The Fortinet unit uses a number of processes to scan files to ensure unwanted files and potential attackers do not get through. The Fortinet unit scans using these antivirus options:

- **File pattern** - The Fortinet will check the file against the file pattern setting you have configured. You can set which file names or file types the Fortinet unit looks for in the incoming traffic.
- **Virus scan** - The virus definitions are kept up to date through the FortiNet Distribution Network. The list is updated on a regular basis so you do not have to wait for a firmware upgrade. Note that you must register the Fortinet unit to and purchase FortiGuard services to use virus scanning through the FDN.

- Grayware - These are unsolicited commercial software programs that are installed on computers, often without the user's consent or knowledge. Grayware programs are generally considered an annoyance, but these programs can cause system performance problems or be used for malicious ends. The Fortinet unit scans for known grayware executable programs in each enabled category.
- Heuristics - The Fortinet heuristic antivirus engine performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results.

The antivirus elements work in sequence to give you an efficient method of scanning incoming files. The first three elements have specific functions, the fourth, the heuristics, is to cover any new previously unknown virus threats. The four elements work together to offer your network unparalleled antivirus protection. To ensure that your system is providing the most protection available, all virus definitions and signatures are up dated regularly through the FortiGuard antivirus services.

To configure the file patterns that the Fortinet scans, go to *UTM > AntiVirus > File Filter*.

To enable grayware blocking, go to *UTM > AntiVirus > Grayware*.

Antivirus settings are turned on in the protection profile. In the protection profile you can enable antivirus options for specific services and which services will use the file patterns as a part of the antivirus process.

To configure antivirus protection profile settings, go to *Firewall > Protection Profile*. Select edit for a profile and select the Anti-Virus options.

For details on the antivirus features and settings, see the [FortiGate Administration Guide](#) or the [Fortinet Online Help](#).

## AntiSpam options

The Fortinet unit's antispam feature detects unsolicited commercial email by identifying spam email messages and spam transmissions from known or suspected spam servers.

This feature requires a FortiGuard subscription and a registered Fortinet unit. When the Fortinet unit receives an email message, it verifies with the FortiGuard server whether it is a valid email or a spam message. FortiGuard Antispam is one of the features designed to manage spam. FortiGuard is an antispam system from Fortinet that includes an IP address black list, a URL black list, and spam filtering tools. The FortiGuard Center accepts submission of spam email messages as well as reports of false positives.

Depending on how you configure the Fortinet unit, it will either tag the message with text so you can easily identify the spam, or delete the message before it reaches the recipient.

The Fortinet unit also enables you to create your own spam filters using banned words and black/white lists.

Banned word lists are specific words that may be typically found in email. The Fortinet unit searches for words or patterns in email messages. If matches are found, values assigned to the words are totalled. If the defined threshold value is exceeded, the message is marked as spam. If no match is found, the email message is passed along to the next filter.

You configure banned words by going to *UTM > Antispam > Banned Word*.

While FortiGuard services maintain a large list of known spammers, it is not perfect. In some cases, some mail tagged as spam is an individual you want to receive mail from, while email that is not caught by the spam filters or users you don't want to receive email from gets through to your inbox.

White lists and black lists enable you to maintain a list of email addresses that you want (white list) or don't want (black list) to receive email from. You can add or remove addresses from lists as required. The Fortinet unit uses both an IP address list and an email address list to filter incoming email, if enabled in the protection profile.

When performing an IP address list check, the Fortinet unit compares the IP address of the message's sender to the IP address list in sequence. If a match is found, the action associated with the IP address is taken. If no match is found, the message is passed to the next enabled spam filter.

When performing an email list check, the Fortinet unit compares the email address of the message's sender to the email address list in sequence. If a match is found, the action associated with the email address is taken. If no match is found, the message is passed to the next enabled antispam filter.

To configure black/white lists, go to *UTM > AntiSpam > E-mail Address*.

You enable antispam options for each mail service (POP3, IMAP and SMTP) in the protection profile. To configure antispam protection profile settings, go to *Firewall > Protection Profile*. Select edit for a profile and select the Spam Filtering options.

For details on the antispam features and settings, see the [FortiGate Administration Guide](#) or the [Fortinet Online Help](#).

## Web filtering

Web filtering is a method of controlling what web sites are viewable by users. There are three main sections to web filtering: the Web Filter Content Block, the URL Filter, and the FortiGuard Web filter. Each interact with each other in such a way as to provide maximum control and protection for the Internet users.

Web filtering options are enabled and configured in the protection profile settings by going to *Firewall > Protection Profile*. Select edit for a profile and selecting either the FortiGuard Web Filtering options or the Web Filtering options. You need to register your Fortinet unit and purchase FortiGuard services to use FortiGuard Web Filtering.

Content blocking enables you to specify file types and words that the Fortinet unit should block when encountered. With web content block enabled, every requested web page is checked against the content block list. The score value of each pattern appearing on the page is added, and if the total is greater than the threshold value set in the protection profile, the page is blocked.

To configure content blocking, go to *UTM > Web Filter > Content Block*.

URL filter enables you to control additional web sites that you can block or allow. This enables you greater control over certain URLs or sub-URLs. The Fortinet unit allows or blocks web pages matching any specified URLs or patterns and displays a replacement message instead.

To configure URL filters, go to *UTM > Web Filter > URL Filter*.

FortiGuard web filtering is a managed web filtering solution provided by Fortinet. FortiGuard web filtering sorts hundreds of millions of web pages into a wide range of categories users can allow, block, or monitor. FortiGuard web filtering includes over 60 million individual ratings of web sites applying to hundreds of millions of pages. Pages are sorted and rated into 56 categories users can allow, block, or monitor. Categories may be added to, or updated, as the Internet evolves. You need to have a FortiGuard subscription to take advantage of FortiGuard web filtering.

For details and configuration options for the web filtering features and settings, see the [FortiGate Administration Guide](#) or the [Fortinet Online Help](#).

## Data leak prevention

FortiGate data leak prevention enables you to stop sensitive data, such as credit card information or social security numbers, from leaving your network. You can define sensitive data patterns and data matching. These patterns will be blocked and/or logged when passing through the FortiGate unit. The data leak prevention system is configured by creating individual rules, combining the rules into a data leak prevention sensor which you can then apply to a protection profile.

While its primary use is to prevent sensitive data from leaving your network, you can also use the data leak prevention to prevent unwanted data from entering your network.

To configure a data leak prevention sensor and pattern, go to *UTM > Data Leak Prevention* and select *Rule* and *Sensor*.

For details and configuration options for data leak prevention, see the [FortiGate Administration Guide](#) or the [Fortinet Online Help](#).

## Application control

Application control is a feature that enables your FortiGate unit to detect and take action against network traffic depending on the application generating the traffic. Based on intrusion protection protocol detectors, application control is a more user-friendly way to use intrusion protection features to log and manage the behavior of application traffic passing through the FortiGate unit. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic even if the traffic uses non-standard ports or protocols.

The FortiGate unit can recognize the network traffic generated by more than 70 applications. You can create application control lists that specify what action will be taken with the traffic of the applications you need to manage.

To configure application control, go to *UTM > Application Control > Control List*.

For details and configuration options for application control see the [FortiGate Administration Guide](#) or the [Fortinet Online Help](#).

## Logging

Logging is an indirect method of protecting your network. The Fortinet unit's robust logging features enable you to see the attacks, spam and virus activity is occurring on your network. Using this information, you can then take the corrective action necessary to resolve any problems before they become major problems.

With alert email, you can configure the Fortinet unit to send alert messages, when specific events occur with specific frequency. By logging to a FortiAnalyzer unit, you can run over 400 reports on various network traffic.

To configure logging, go to *Log&Report > Log Config*.

For details and configuration options for the logging features and settings, see the [FortiGate Administration Guide](#) or the [Fortinet Online Help](#).

# Fortinet Firmware

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

You can also use the instructions in this chapter to downgrade, or revert, to a previous version. The Fortinet unit includes a number of firmware installation options that enables you to test new firmware without disrupting the existing installation, and load it from different locations as required.

In addition to firmware images, Fortinet issues patch releases--maintenance release builds that resolve important issues. Fortinet strongly recommends reviewing the release notes for the patch release, as well as testing and reviewing the patch release before upgrading the firmware. Follow the steps below:

- download and review the release notes for the patch release
- download the patch release
- back up the current configuration
- install the patch release using the procedure “[Testing new firmware before installing](#)” on page 43
- test the patch release until you are satisfied that it applies to your configuration.

Installing a patch release without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Only Fortinet admin user and administrators whose access profiles contain system read and write privileges can change the Fortinet firmware.

This section includes the following topics:

- [Downloading firmware](#)
- [Using the web-based manager](#)
- [Using the CLI](#)
- [Installing firmware from a system reboot using the CLI](#)
- [Testing new firmware before installing](#)

## Downloading firmware

Firmware images for all Fortinet units is available on the Fortinet Customer Support web site. You must register your Fortinet unit to access firmware images. Register the Fortinet unit by visiting <http://support.fortinet.com> and select Product Registration.

### To download firmware

- 1 Log into the site using your user name and password.
- 2 Go to *Firmware Images > FortiGate*.
- 3 Select the most recent FortiOS version.
- 4 Locate the firmware for your Fortinet unit, right-click the link and select the Download option for your browser.



**Note:** Always review the [Release Notes](#) for a new firmware release before installing. The [Release Notes](#) can include information that is not available in the regular documentation.

# Using the web-based manager

## Upgrading the firmware

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 upgrade the firmware

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

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

## Reverting to a previous version

The following procedures revert the Fortinet unit to its factory default configuration and deletes any configuration settings.

Before beginning this procedures, ensure you back up the Fortinet unit configuration.

If you are reverting to a previous FortiOS version, 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 more information, 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

- 1 Copy the firmware image file to the management computer.
- 2 Log into the Fortinet 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 Fortinet unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the Fortinet login. This process takes a few minutes.

- 7 Log into the web-based manager.

## 8 Restore your configuration.

For information about restoring your configuration see “[Restoring a configuration](#)” on [page 24](#).

## Backup and Restore from a USB key

Use a USB key to either backup a configuration file or restore a configuration file. You should always make sure a USB key is properly install before proceeding since the Fortinet 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. An encrypted file is ineffective if selected for the USB Auto-Install feature.

### To backup configuration

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

### To restore configuration

- 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*.

## Using the USB Auto-Install

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 Fortinet unit.



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



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

### To configure the USB Auto-Install

- 1 Go to *System > Maintenance > Backup and Restore*.
- 2 Select the Expand 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 file names 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*.

## Using the CLI

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 more information, see the *FortiGate Administration Guide*.

Before you begin, ensure you have a TFTP server running and accessible to the Fortinet unit.

### 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 Fortinet 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 Fortinet unit:

```
execute restore image tftp <filename> <tftp_ipv4>
```

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

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

The Fortinet unit responds with the message:

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

- 6 Type `y`.  
The Fortinet unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.
- 7 Reconnect to the CLI.
- 8 Update antivirus and attack definitions, by entering:

```
execute update-now
```

### Reverting to a previous version

This procedure reverts the Fortinet 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 Fortinet 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

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. 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 Fortinet 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 Fortinet CLI.
- 4 Make sure the Fortinet unit can connect to the TFTP server.

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

```
execute ping 192.168.1.168
```

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

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

Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is `imagev28.out` and the IP address of the TFTP server is 192.168.1.168, enter:

```
execute restore image tftp image28.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 Fortinet unit uploads the firmware image file. After the file uploads, a message similar to the following appears:

```
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 Fortinet 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 restore your previous configuration, if needed, use the command:

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

**10** Update antivirus and attack definitions using the command:

```
execute update-now.
```

## Installing firmware from a system reboot using the CLI

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

To use this procedure, you must connect to the CLI using the Fortinet console port and a RJ-45 to DB-9, or null modem cable.

This procedure reverts the Fortinet unit to its factory default configuration.

For this procedure you install a TFTP server that you can connect to from the Fortinet internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, ensure you back up the Fortinet unit configuration.

If you are reverting to a previous FortiOS version, 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 or null modem cable.**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 Fortinet 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
```

**6** Enter the following command to restart the Fortinet unit.

```
execute reboot
```

The Fortinet unit responds with the following message:

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

**7** Type `y`.

As the Fortinet unit starts, a series of system startup messages appears. When the following messages appears:

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 Fortinet unit reboots and you must log in and repeat the `execute reboot` command.

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

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[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 Fortinet 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]:
```

**11** Enter the firmware image filename and press Enter.

The TFTP server uploads the firmware image file to the Fortinet unit and a message similar to the following appears:

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

**12** Type D.

The Fortinet 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 <interface>
    set ip <address_ip4mask>
    set allowaccess {ping|https|ssh|telnet|http}
  end
```

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

## Backup and Restore from a USB key

Use a USB key to either backup a configuration file or restore a configuration file. You should always make sure a USB key is properly install before proceeding since the Fortinet 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. An encrypted file is ineffective if selected for the USB Auto-Install feature.

### 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 Fortinet 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

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 Fortinet unit.



**Note:** You need an unencrypted configuration file for this feature. Also the default files, `image.out` and `system.conf`, must be in the root directory of the USB key.



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

### 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 a USB key

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

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



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

## Testing new firmware before installing

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 Fortinet unit operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the Fortinet 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 the firmware” on page 36](#).

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

For this procedure you install a TFTP server that you can connect to from the Fortinet 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 or null modem cable.
- 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 use the following command to ping the computer running the TFTP server. For example, if the TFTP server’s IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to restart the Fortinet unit:

```
execute reboot
```

- 6 As the Fortinet unit reboots, press any key to interrupt the system startup. As the Fortinet unit starts, a series of system startup messages appears. When the following messages appears:

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

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



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

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

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[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 of the Fortinet unit to connect to the TFTP 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 Fortinet unit and the following appears.

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

## 12 Type R.

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

You can test the new firmware image as required. When done testing, you can reboot the Fortinet unit, and the Fortinet unit will resume using the firmware that was running before you installed the test firmware.

# Index

## A

- adding a default route, 17
- admin password, 26
- air flow, 7
- ambient temperature, 7
- antispam options, 32
- antivirus options, 31
- auto-install, 37
- auto-install from CLI, 42

## B

- backing up, 23

## C

- certificate, security, 12
- CLI, 13
  - upgrading the firmware, 38
- comments, documentation, 4
- configure
  - backup, 23
  - DNS, 16, 21
  - FortiGuard, 27
  - interfaces, 14
  - restore, 24
- connecting
  - to the CLI, 13
  - web-based manager, 12
- customer service, 3

## D

- date and time, 25
- default
  - adding a route, 17
- default route, 17
- DHCP, 15
- DNS override, 14
- documentation
  - commenting on, 4
  - Fortinet, 4
- domain name server
  - configure, 21
- domain name server, configure, 16
- downloading firmware, 35

## E

- earthing, 8
- execute shutdown, 9

## F

- firewall policies, 18, 30

## firmware

- backup and restore from USB, 42
- download, 35
- from system reboot, 40
- installing, 40
  - re-installing current version, 41
- restore from CLI, 41
- restoring previous config, 41
- revert from CLI, 38
- reverting with web-based manager, 36
- testing before use, 43
- testing new firmware, 43
- upgrade from CLI, 38
- upgrade with web-based manager, 36
- upgrading using the CLI, 38

FortiGate documentation

- commenting on, 4

FortiGuard, 27

Fortinet customer service, 3

Fortinet documentation, 4

Fortinet Knowledge Center, 4

## G

- gateway, 17
- grounding, 8

## H

- humidity, 7

## I

- Initial Disc Timeout, 15
- interface, configuring, 14
- introduction
  - Fortinet documentation, 4

## L

- logging, 34

## M

- management IP, 20

## N

- NAT mode, 11

## O

- operating temperature, 7

## P

- PADT timeout, 15
- password, changing, 26
- power off, 9
- protection profiles, 29

**R**

restore, 24  
restoring  
    previous firmware configuration, 41  
reverting firmware, 36

**S**

security certificate, 12  
shielded twisted pair, 8  
shut down, 9  
signatures, update, 27  
static route, 17  
system reboot, installing, 40

**T**

technical support, 3  
TFTP server, 40  
time and date, 25

time zone, 25  
Transparent mode, 12  
    switching to, 20

**U**

unnumbered IP, 15  
update signatures, 27  
updating  
    antivirus and IPS, web-based manager, 27  
upgrading  
    firmware using the CLI, 38  
USB, 42  
    auto-install, 37, 42  
    CLI commands, 43  
    key, 37

**W**

web filtering, 33  
web-based manager, 12



**FORTINET**<sup>®</sup>

[www.fortinet.com](http://www.fortinet.com)

**FORTINET**<sup>®</sup>

[www.fortinet.com](http://www.fortinet.com)