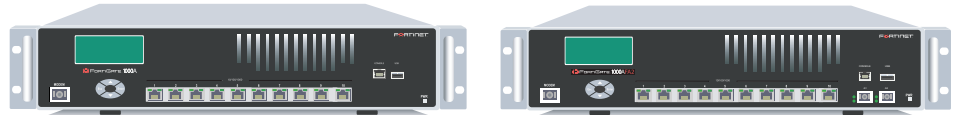


# FortiGate-1000A / 1000AFA2 normal operating LED indicators

LED	State	Description
PWR	Green	The FortiGate unit is on.
Ports 1 to 10	Green	The correct cable is connected to the copper 10/100/1000 interface and the connected equipment has power.
	Flashing	Network activity at this interface.
	Amber	The interface is connected at 1000 Mbps.
Ports A1 and A2 (1000AFA2)	Green	The correct optical fiber patch cable is connected to the gigabit fiber interface.
	Flashing	Network activity at the gigabit fiber interface.

# FORTINET FortiGate-1000A / 1000AFA2



# QuickStart Guide

© Copyright 2005 Fortinet Incorporated. All rights reserved.

### Trademarks

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

### Regulatory Compliance

FCC Class A Part 15 CSA/CUS

16 November 2005

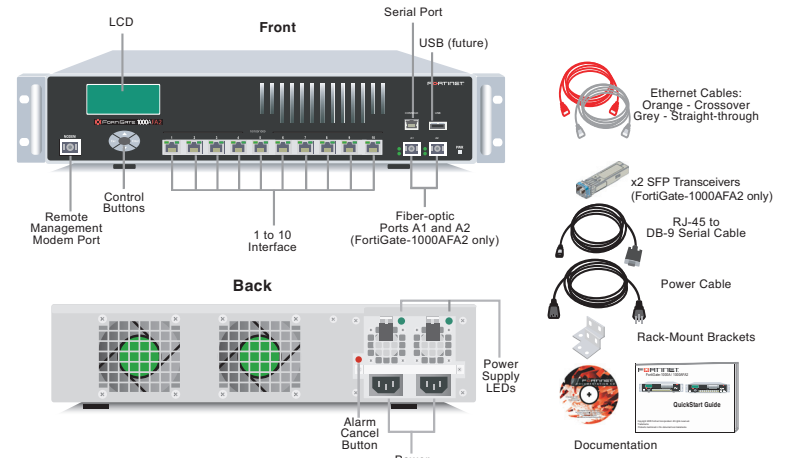
For technical support please visit <http://www.fortinet.com>.

01-28011-0258-20051116

## 1 Checking the package contents

Check that the package contents are complete. FortiGate-1000AFA2 shown.

Connector	Type	Speed	Protocol	Description
Ports 1 to 10	RJ-45	1000Base-T	Ethernet	Copper gigabit connection to 10/100/1000 copper networks.
Ports A1 and A2 (1000AFA2)	LC SFP	1000Base-SX	Ethernet	Multimode fiber optic connections to gigabit optical networks for small packet performance required for voice, video and other multimedia streaming applications.
CONSOLE	RJ-45	9600 bps	RS-232 serial	Serial connection to the command line interface.

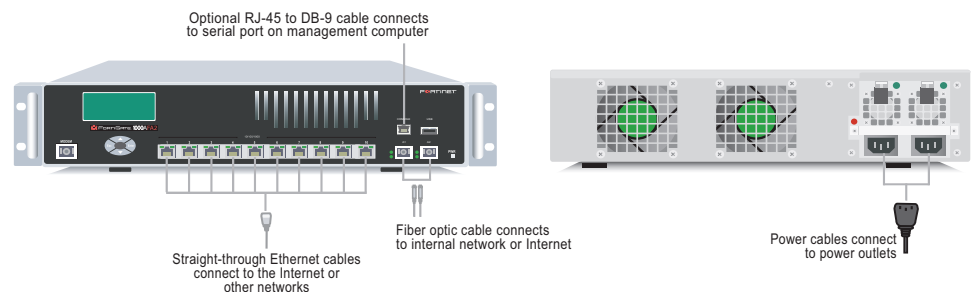


## 2 Connecting the FortiGate unit

Connect the FortiGate-1000A / 1000AFA2 unit to a power outlet and to the internal and external networks. The FortiGate-1000AFA2 is shown in the diagram.

- Mount the unit in a standard 19-inch rack. It requires 2 U of vertical space in the rack.
- Make sure the power is not connected or off before connecting the power and network cables.
- MAIN MENU appears when the unit is up and running.

If only one power supply is connected, an audible alarm sounds to indicate a failed power supply. To stop this alarm, press the red alarm cancel button.



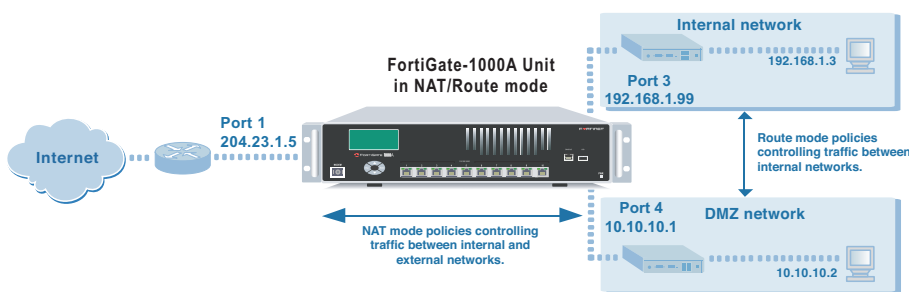
## 3 Planning the configuration

Before beginning to configure the FortiGate-1000A or FortiGate-1000AFA2, you need to plan how to integrate the unit into your network. Your configuration plan is dependent upon the operating mode that you select: NAT/Route mode (the default) or Transparent mode.

### NAT/Route mode

In NAT/Route mode, the FortiGate unit is visible to the networks that it is connected to. All of its interfaces are on different subnets. Each interface that is connected to a network must be configured with an IP address that is valid for that network.

You would typically use NAT/Route mode when the FortiGate unit is deployed as a gateway between private and public networks. In its default NAT/Route mode configuration, the unit functions as a firewall. Firewall policies control communications through the FortiGate unit. No traffic can pass through the FortiGate unit until you add firewall policies.



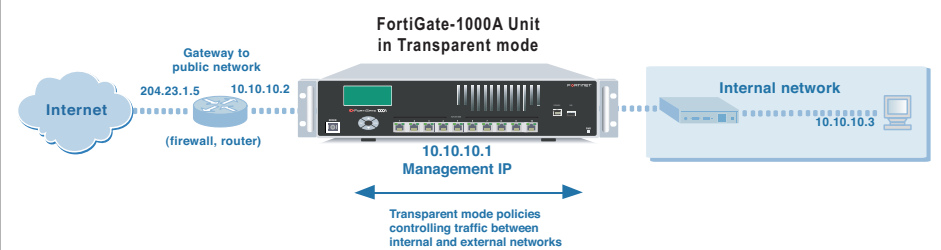
In NAT/Route mode, firewall policies can operate in NAT mode or in Route mode. In NAT mode, the FortiGate unit performs network address translation before IP packets are sent to the destination network. In route mode, no translation takes place.

Refer to the Documentation CD-ROM for information on how to control traffic, and how to configure HA, antivirus protection, Web content filtering, Spam filtering, intrusion prevention (IPS), and virtual private networking (VPN).

### Transparent mode

In Transparent mode, the FortiGate unit is invisible to the network. All of its interfaces are on the same subnet. You only have to configure a management IP address so that you can make configuration changes.

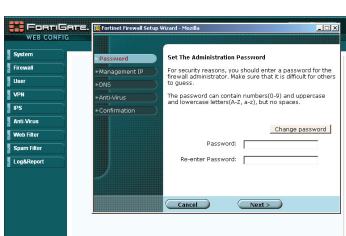
You would typically use the FortiGate unit in Transparent mode on a private network behind an existing firewall or behind a router. In its default Transparent mode configuration, the unit functions as a firewall. No traffic can pass through the FortiGate unit until you add firewall policies.



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

## 4 Choosing a configuration tool

Choose between two different tools to configure the FortiGate unit.



### Web-based manager and Setup Wizard

Using the Setup Wizard you can configure basic configuration settings by stepping through the wizard pages and filling in the information required. The FortiGate web-based manager is an easy to use management tool.

Use it to configure the administrator password, interface addresses, the default gateway address, and the DNS server addresses. To configure advanced settings, see the online help and Documentation CD-ROM.

#### Requirements:

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

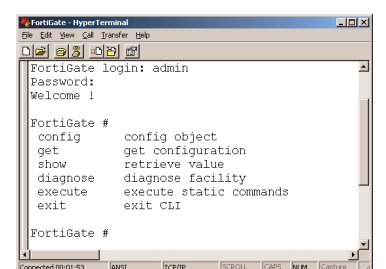
### Command Line Interface (CLI)

The CLI is a full-featured management tool.

Use it to configure the administrator password, the interface addresses, the default gateway address, and the DNS server addresses. To configure advanced settings, see the *FortiGate CLI Reference Guide* on the Documentation CD-ROM.

#### Requirements:

- The serial connection between the FortiGate unit and a management computer.
- A terminal emulation application (HyperTerminal for Windows) on the management computer.



# 5 Collecting information

Use these tables to record your FortiGate-1000A or FortiGate-1000AFA2 configuration. You can record NAT/Route or Transparent mode settings and general settings that apply to both modes.

## NAT/Route mode

Port 1	IP: _____ Netmask: _____
Port 2	IP: _____ Netmask: _____
Port 3	IP: _____ Netmask: _____
Port 4	IP: _____ Netmask: _____
Port 5	IP: _____ Netmask: _____
Port 6	IP: _____ Netmask: _____
Port 7	IP: _____ Netmask: _____
Port 8	IP: _____ Netmask: _____
Port 9	IP: _____ Netmask: _____

Port 10	IP: _____ Netmask: _____
Port A1 (FortiGate-1000AFA2)	IP: _____ Netmask: _____
Port A2 (FortiGate-1000AFA2)	IP: _____ Netmask: _____

## Transparent mode

Management IP:	IP: _____ Netmask: _____
----------------	-----------------------------

The management IP address and netmask must be valid for the network that the FortiGate unit is connected to.

## General settings

Administrator password:	_____
Network Settings:	Default Gateway: _____
	Primary DNS Server: _____
	Secondary DNS Server: _____

A default gateway is required for the FortiGate unit to route connections to the Internet.

# 6 Configuring the FortiGate unit

## Web-based manager and Setup Wizard

### NAT/Route mode

#### Using the Setup Wizard

To configure the FortiGate unit using the Setup Wizard, select the Easy Setup Wizard button and follow the prompts.



#### Using the web-based manager

##### To change the administrator password

- Go to **System > Admin > Administrators**.
- Select Change Password for the admin administrator and enter a new password.

##### To configure interfaces

- Go to **System > Network > Interface**.
- Select the edit icon for each interface to configure.
- Set the addressing mode for the interface. (see the online help for information.)
  - For manual addressing, enter the IP address and netmask for the interface.
  - For DHCP addressing, select DHCP and any required settings.
  - For PPPoE addressing, select PPPoE, and enter the username and password and any other required settings.

##### To configure the Primary and Secondary DNS server IP addresses

- Go to **System > Network > DNS**, enter the Primary and Secondary DNS IP addresses that you recorded above and select Apply.

##### To configure a Default Gateway

- Go to **Router > Static** and select Edit icon for the static route.
- Set Gateway to the Default Gateway IP address that you recorded above and select OK.

**Note:** If you change the IP address of Port 1 (NAT/Route mode) or management IP address (Transparent mode), you must use this address to reconnect to the web-based manager and Setup Wizard. You might also have to change the IP address of the management computer to be on the same subnet as the new IP address.

- Connect Port 1 to the same network as a management computer.
- Configure the management computer to be on the same subnet as Port 1. To do this, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
- To access the FortiGate web-based manager, start Internet Explorer and browse to https://192.168.1.99 (remember to include the "s" in https://).
- Type admin in the Name field and select Login.

### Transparent mode

#### To switch from NAT/route mode to transparent mode

- Go to **System > Status**, select Change beside Operation Mode, and select OK.
- Change the IP address of the management computer to 10.10.10.2 and use Internet Explorer to browse to https://10.10.10.1.

#### Using the Setup Wizard

To configure the FortiGate unit using the Setup Wizard, select the Easy Setup Wizard button and follow the prompts.

#### Using the web-based manager

##### To change the administrator password using the web-based manager

- Go to **System > Admin > Administrators**.
- Select Change Password for the admin administrator and enter a new password.

##### To configure the management interface using the web-based manager

- Go to **System > Network > Management**.
- Enter the Management IP address and netmask that you recorded above.
- Select administrative access options if required and select OK.

##### To configure the Primary and Secondary DNS server IP addresses

- Go to **System > Network > DNS**, enter the Primary and Secondary DNS IP addresses that you recorded above and select Apply.

##### To configure a Default Gateway

- Go to **System > Network > Management**.
- Set Default Gateway to the Default Gateway IP address that you recorded above and select OK.

# Using the Command Line Interface

## NAT/Route mode

- Configure Port 1.
 

```
config system interface
    edit port1
        set mode static
        set ip <intf_ip> <netmask_ip>
    end
```
- Repeat to configure each interface, for example, to configure Port 2:
 

```
config system interface
    edit port2
        set mode static
        set ip <intf_ip> <netmask_ip>
    end
```
- Configure the primary and secondary DNS server IP addresses.
 

```
config system dns
    set primary <dns-server_ip>
    set secondary <dns-server_ip>
    end
```
- Configure the default gateway.
 

```
config router static
    edit 1
        set gateway <gateway_ip>
    end
```

- Use the RJ-45 to DB-9 cable to connect the FortiGate Console port to the management computer serial port.
- Start a terminal emulation program (HyperTerminal) on the management computer. Use these settings: Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
- At the Login: prompt, type admin and press Enter twice (no password required).

## Transparent mode

- Change from NAT/Route mode to Transparent mode.
 

```
config system global
    set opmode transparent
    end
```
- Wait a moment and then log in again at the prompt.
- Configure the Management IP address.
 

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

Configure the DNS server IP address.

```
config system dns
    set primary <dns-server_ip>
    set secondary <dns-server_ip>
    end
```
- Configure the default route.
 

```
config router static
    edit 1
        set gateway <gateway_ip>
    end
```

# 7 Completing the configuration

Congratulations!

You have finished configuring the basic settings. Your network is now protected from Internet-based threats. To explore the full range of configuration options, see the online help or the Documentation CD-ROM.

## Restarting the FortiGate unit

Should you mistakenly change a network setting and cannot connect to the unit, reboot the unit and try again or to set the unit back to factory defaults and start over again.

- To restart the unit, go to **System > Maintenance > ShutDown** and select Reboot. CLI: `execute reboot`
- To reset the unit, go to **System > Maintenance > ShutDown** and select Reset to factory default. CLI: `execute factoryreset`