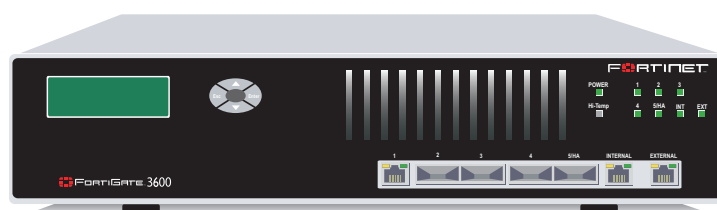


LED	State	Description
Power	Green	The FortiGate unit is on.
	Off	The FortiGate unit is off.
Display Panel LEDs: 1, 2, 3, 4 5/HA, INT, EXT	Green	The correct cable is in use and the connected equipment has power.
	Flashing Green	Network activity at this interface.
	Off	No link established.
Port 1	Amber	The link is up.
	Flashing Amber	Network activity at this interface.
	Green	Link speed is 100Mb/s
	Off	Link speed is 10Mb/s
Internal, External	Amber	The link is up.
	Flashing Amber	Network activity at this interface.
	Green	Link speed is 1000Mb/s
	Off	Link speed is 100Mb/s

# QuickStart Guide



FortiGate-3600

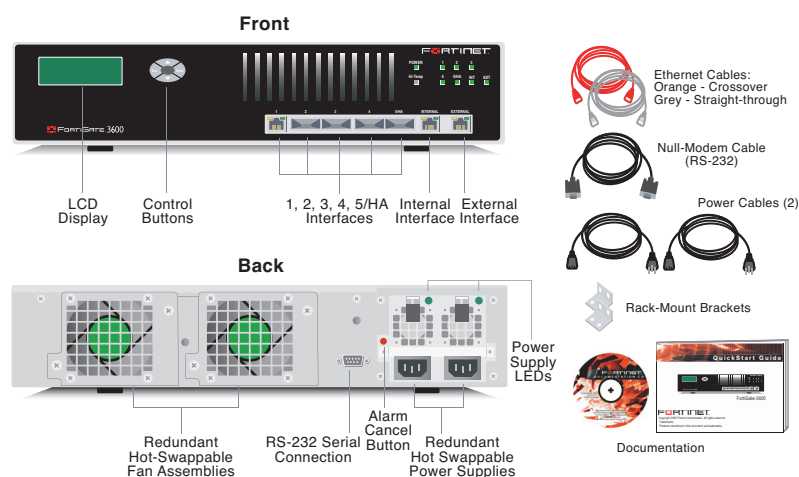


© Copyright 2009 Fortinet Incorporated. All rights reserved.  
 Products mentioned in this document are trademarks or registered trademarks of their respective holders.  
 Regulatory Compliance  
 FCC Class A Part 15 CSA/CUS  
 23 January 2009

01-30006-0041-20090123

## 1 Checking the Package Contents

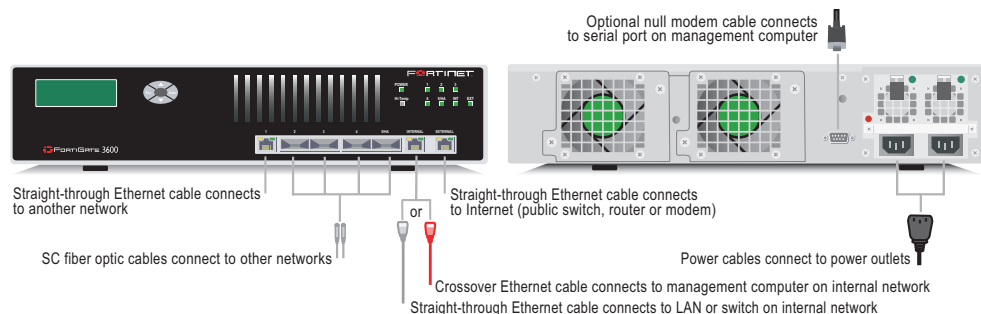
Connector	Type	Speed	Protocol	Description
Internal	SC	1000Base-SX	Ethernet	Copper gigabit connection to the internal network.
External	SC	1000Base-SX	Ethernet	Copper gigabit connection to the internet.
Port 1	RJ-45	10/100Base-T	Ethernet	Optional connection to a 10/100Base-T network.
Port 2 to 4	SC	1000Base-SC	Ethernet	Optional multimode fiber optic connections to other networks.
Port 5/HA	SC	1000Base-SC	Ethernet	Optional multimode fiber optic connection to another network, or to other FortiGate-3600 units for high availability (HA).
CONSOLE	DB-9	9600 bps	RS-232 serial	Optional connection to the management computer. Provides access to the command line interface (CLI).



## 2 Connecting

Connect the FortiGate unit to a power outlet and to the internal and external networks.

- Place the unit on a stable surface.
- The FortiGate unit requires 1.5 inches (3.75 cm) clearance above and on each side to allow for cooling.
- Make sure the power switch on the back of the unit is turned 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

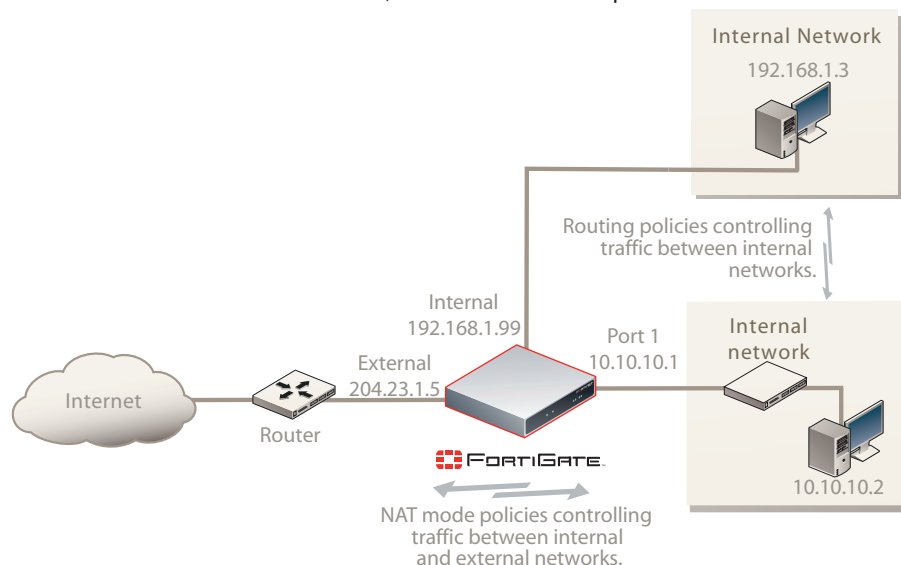
Before beginning to configure the FortiGate unit, you need to plan how to integrate the unit into your network. Your configuration plan is dependent upon the operating mode that you select: NAT/Route mode (the default) or Transparent mode. Refer to the Documentation CD-ROM for information on how to control traffic, and how to configure HA, antivirus protection, FortiGuard, Web content filtering, Spam filtering, intrusion prevention (IPS), and virtual private networking (VPN).

### NAT/Route mode

In NAT/Route mode, each FortiGate unit is visible to the network that it is connected to. All of its interfaces are on different subnets. Each interface 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.

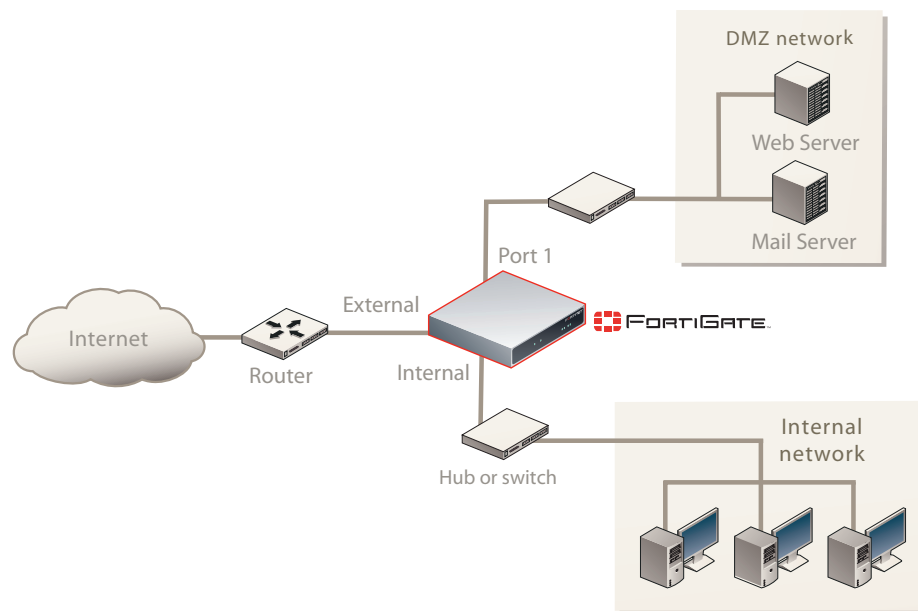


### Transparent mode

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 four network segments to the FortiGate unit to control traffic between these network segments.



# 4 Choosing a Configuration Tool

## Web-based manager

The FortiGate web-based manager is an easy to use management tool. Use it to configure the administrator password, the interface and default gateway addresses, and the DNS server addresses.

### Requirements:

- An Ethernet connection between the FortiGate unit and management computer.
- Internet Explorer 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 Documentation CD-ROM.

### Requirements:

- The DB-9 serial connection between the FortiGate unit and management computer.
- A terminal emulation application (HyperTerminal for Windows) on the management computer.

# 5 Collecting Information

## NAT/Route Mode

Internal	IP:	_____
	Netmask:	_____
External	IP:	_____
	Netmask:	_____
Port 1	IP:	_____
	Netmask:	_____
Port 2	IP:	_____
	Netmask:	_____
Port 3	IP:	_____
	Netmask:	_____
Port 4	IP:	_____
	Netmask:	_____
Port 5/HA	IP:	_____
	Netmask:	_____

The internal interface IP address and netmask must be valid for the internal network.

## Transparent mode

Management IP	IP:	_____
	Netmask:	_____

The management IP address and netmask must be valid for the network from which you will manage the FortiGate unit.

## 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.

## Factory default settings

NAT/Route mode		Transparent mode	
Internal interface	192.168.1.99	Management IP	0.0.0.0
External interface	192.168.100.99	<b>Administrative account settings</b>	
Ports 1 to 5	0.0.0.0	User name	admin
		Password	(none)
DHCP server on Internal interface	192.168.1.110 – 192.168.1.210		

# 6 Configuring the FortiGate Unit

## Web-based Manager

1. Connect the FortiGate internal interface to a management computer Ethernet interface. Use a cross-over Ethernet cable to connect the devices directly. Use straight-through Ethernet cables to connect the devices through a hub or switch.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiGate unit. To do this, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
3. 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://).
4. Type admin in the Name field and select Login.

## NAT/Route mode

### To change the administrator password

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

### To configure interfaces

1. Go to **System > Network > Interface**.
2. Select the edit icon for each interface to configure.
3. 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

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

### To configure a Default Gateway

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

## Transparent mode

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

1. Go to **System > Config > Operation Mode** and select Transparent.
2. Set the Management IP/Netmask to 192.168.1.99/24.
3. Set a default Gateway and select Apply.

### To change the administrator password

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

### To change the management interface

1. Go to **System > Config > Operation Mode**.
2. Enter the Management IP address and netmask that you recorded above and select Apply.

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

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

## Command Line Interface

1. Use the DB9 serial cable to connect the FortiGate Console port to the management computer serial port.
2. Start a terminal emulation program (HyperTerminal) on the management computer. Use these settings:
3. Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
4. At the Login: prompt, type admin and press Enter twice (no password required).

## NAT/Route mode

1. Configure the FortiGate internal interface.
 

```
config system interface
  edit internal
    set ip <intf_ip>/<netmask_ip>
  end
```
2. Repeat to configure each interface, for example, to configure the WAN1 interface.
 

```
config system interface
  edit wan1
    ...
```
3. Configure the primary and secondary DNS server IP addresses.
 

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

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

## Transparent Mode

1. Change from NAT/Route mode to Transparent mode and configure the Management IP address.
 

```
config system settings
  set opmode transparent
  set ip <mng_ip>/<netmask>
  set gateway <gateway_ip>
end
```
2. Configure the DNS server IP address.
 

```
config system dns
  set primary <dns-server_ip>
  set secondary <dns-server_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.

Visit these links for more information and documentation for your Fortinet product.

- Technical Documentation - <http://docs.forticare.com>
- Fortinet Knowledge Center - <http://kc.forticare.com>
- Fortinet Technical Support - <http://support.fortinet.com>