LED	State	Description
Power	Green	The FortiGate unit is on.
	Off	The FortiGate unit is off.
Status	Green	The FortiGate unit is running normally.
	Off	The FortiGate unit is off.
MGMT1 and MGMT2 (Right LED)	Green	The correct cable is in use and the connected equipment has power.
	Flashing Green	Network activity at this interface.
	Off	No link established.
MGMT1 and MGMT2 (Left LED)	Green	Connection at 1000 Mb.
	Amber	Connection at 100 Mb.
	Off	Connection at 10 Mb.
Ports 1 to 16	Green	The correct cable is in use and the connected equipment has power.
	Flashing Green	Network activity at this interface.
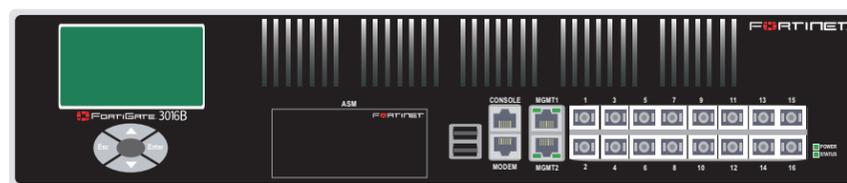
FortiGate-3016B

FORTINET™

01-30006-0402-20080328

1 Checking the Package Contents

Connector	Type	Speed	Protocol	Description
MGMT1 and MGMT2	RJ-45	10/100/1000 Base-T	Ethernet	Copper gigabit connection to 10/100/1000 copper networks.
Ports 1 to 16	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 8/N/1	RS-232 serial	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB	USB		USB	Optional connection to a USB key for firmware backup and installation.

Front

LCD Display
Control Buttons
USB
Serial and Modem Connections
Copper Management Ports
Fiber Ports

Back

Power Connections

Ethernet Cables:
Orange - Crossover
Grey - Straight-through

RJ-45 to DB-9 Serial Cable   Power Cables (2)

4x Optical Transceivers
4x Copper Transceivers

Rack-Mount Brackets

Documentation
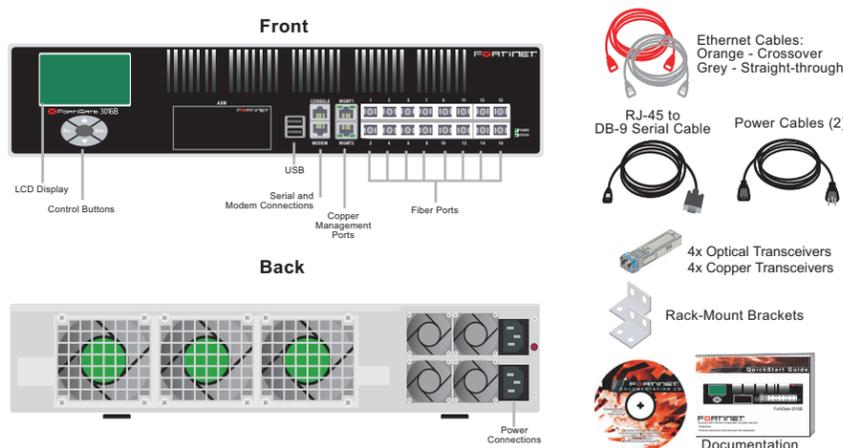
2 Connecting

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

- Place the unit on a stable surface.

- Connect both power cables into the back of the FortiGate unit, then plug the power cables into a power bar.

- 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.

Optional RJ-45 to DB-9 cable connects to serial port on management computer

Straight-through Ethernet for access to the web-based manager

Fiber optic cable connects to internal network or Internet

Power alarm reset bu

Power cables connect to power outlets
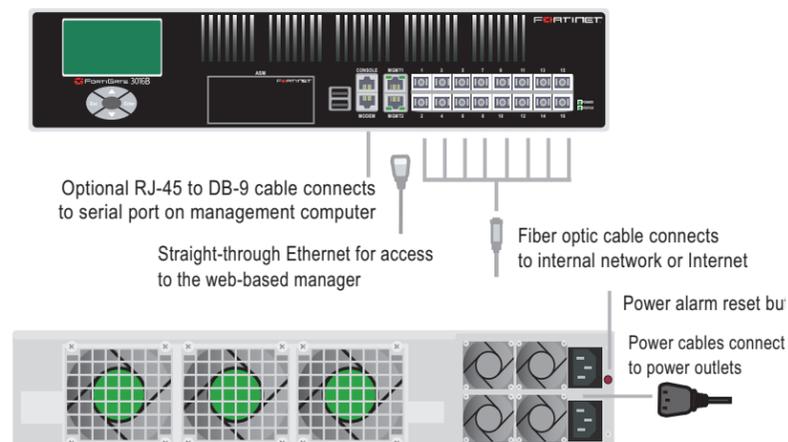
3 Planning the Configuration

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.

Internal Network
192.168.1.3

Routing policies controlling traffic between internal networks.

Internal network

Port 2
192.168.1.99
Port 3
10.10.10.1
Port 1
204.23.1.5

Internet
Router

FortiGate

10.10.10.2

NAT mode policies controlling traffic between internal and external networks.
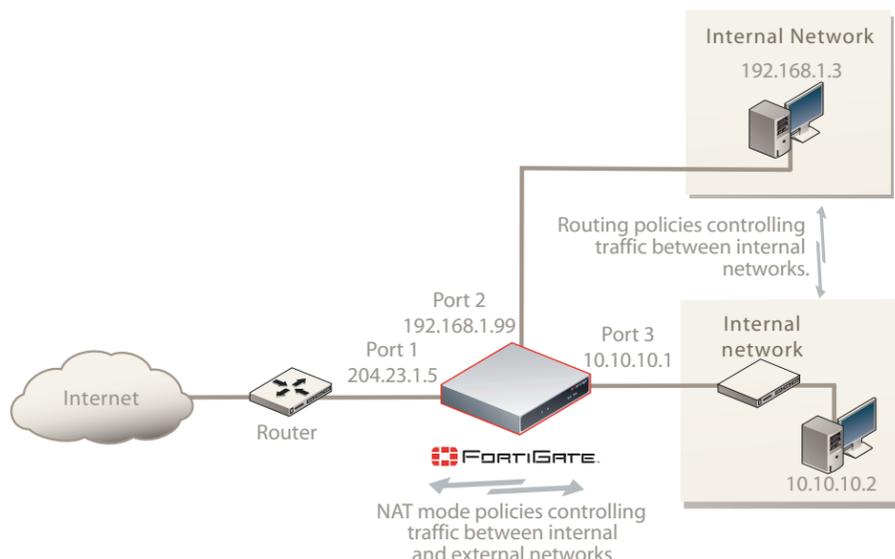
Transparent mode

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.

DMZ network

Web Server

Mail Server

Port 3

Poirt 1

Internet
Router

FortiGate

Port 2

Hub or switch

Internal network
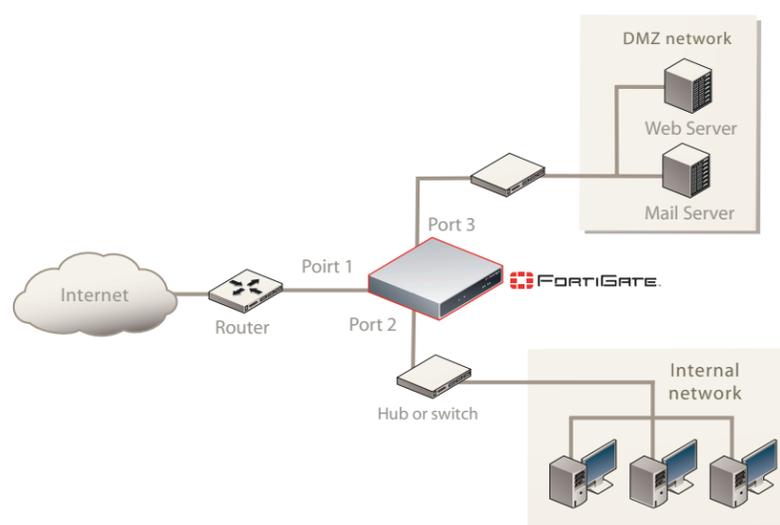
4 Choosing a Configuration Tool

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, default gateway address, and DNS server addresses. To configure advanced settings, see the *CLI Reference* on the Tools and Documentation CD.

Requirements:
• The RJ-45 to 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

MGMT 1	IP:	_____.____.____.____	Port 8	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____
MGMT 2	IP:	_____.____.____.____	Port 9	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____
Port 1	IP:	_____.____.____.____	Port 10	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____
Port 2	IP:	_____.____.____.____	Port 11	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____
Port 3	IP:	_____.____.____.____	Port 12	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____
Port 4	IP:	_____.____.____.____	Port 13	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____
Port 5	IP:	_____.____.____.____	Port 14	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____
Port 6	IP:	_____.____.____.____	Port 15	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____
Port 7	IP:	_____.____.____.____	Port 16	IP:	_____.____.____.____
	Netmask:	_____.____.____.____		Netmask:	_____.____.____.____

Transparent mode

Management IP	IP:	_____.____.____.____
	Netmask:	_____.____.____.____

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	
MGMT 1	192.168.1.99	Management IP	0.0.0.0
MGMT 2	192.168.2.99	**Administrative account settings**	
Ports 1 to 16	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 RJ-45 to 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 <port_num>
           set ip <intf_ip>/<netmask_ip>
           set allowaccess {http|https|ssh|ping|snmp|telnet}
   end
   ```

2. Configure the primary and secondary DNS server IP addresses.
   ```
   config system dns
       set primary <dns-server_ip>
       set secondary <dns-server_ip>
   end
   ```

3. 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 manageip <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 Tools and Documentation CD.

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