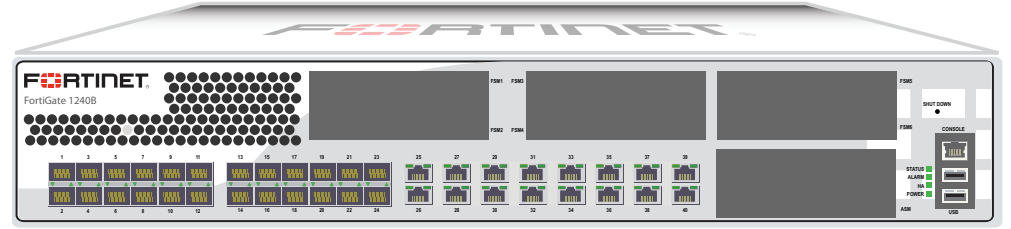


LED	State	Description	
Power	Green	The unit is on.	
	Off	The unit is off.	
Status	Green flashing	The unit is starting up.	
	Green	The unit is running normally.	
HA	Yellow	The unit being used in an HA cluster.	
Alarm		To be supported in a future release.	
Ports 1 to 24	Link	Green	Port is online.
		Off	Port is offline.
	Activity	Green blinking	Port is receiving or sending data.
		Off	Port might be on but is not receiving or sending data.
Ports 25 to 40	Link	Green	Port is online.
		Flashing	Port is receiving or sending data.
	Activity	Green	Connected at 1000Mbps.
		Amber	Connected at 100 Mbps.
		Off	Connected at 10 Mbps.
AC power	Green	AC cable is connected and has power.	
	Amber	AC cable is not connected or does not have power.	
Fan	Green	The fan is running and the speed is within proper range.	
	Off	The fan is not running or the speed is over threshold.	

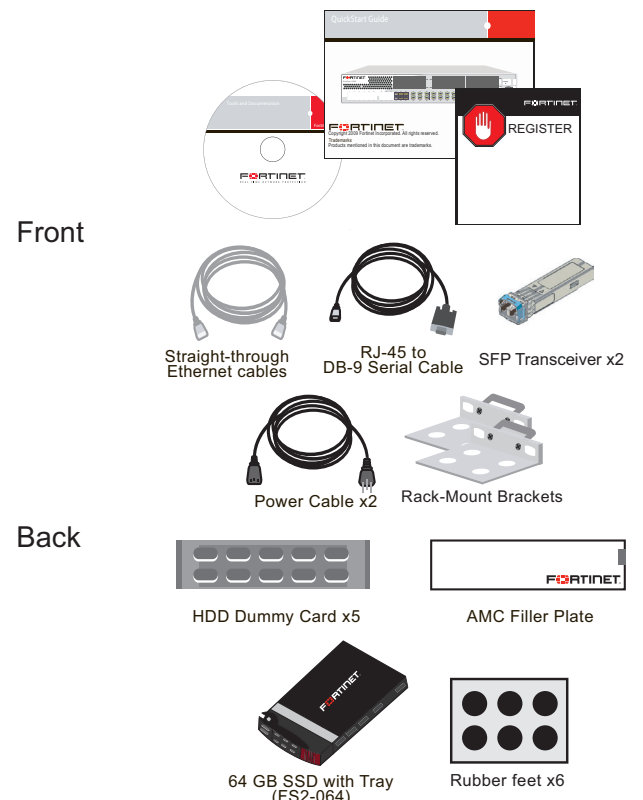
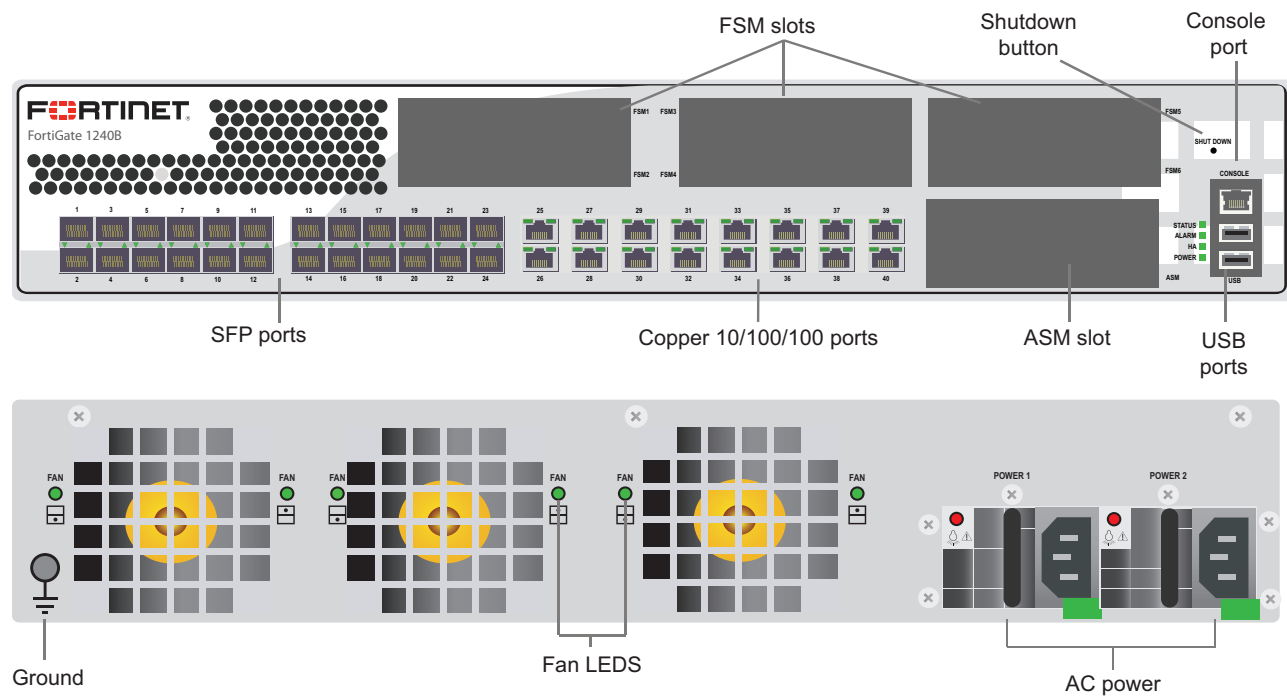


© Copyright 2009 Fortinet Incorporated. All rights reserved.  
 Products mentioned in this document are trademarks or registered trademarks of their respective holders.  
 Regulatory Compliance  
 FCC Class A Part 15 CSA/CUS  
 17 November 2009

01-30007-106971-20091117

## Package Contents

Interface	Type	Speed	Protocol	Description
Ports 1 to 24	SFP	1 Gbps/auto	Ethernet	Small form-factor pluggable transceiver (SX-SFP) supports 1 Gbps for SERDES and auto mode for SGMII modes (NP Accelerated).
Ports 25 to 38	RJ-45	10/100/1000	Ethernet	Copper gigabit connection to 10/100/1000 copper networks (NP accelerated).
Ports 39 to 40	RJ-45	10/100/1000	Ethernet	Two management ports.
CONSOLE	RJ-45	9600 bps	RS-232 serial	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB	USB			Two USB ports for optional connection to a USB key for firmware backup and installation.
FSM slot	FSM			Six SATA hard disk drive slots supports 2.5 inch solid state drives.
AMC slot	AMC			One single-width AMC slot supports all Fortinet ASM modules.
Shutdown button				When pressed, the RAID system shuts down.



## Connecting

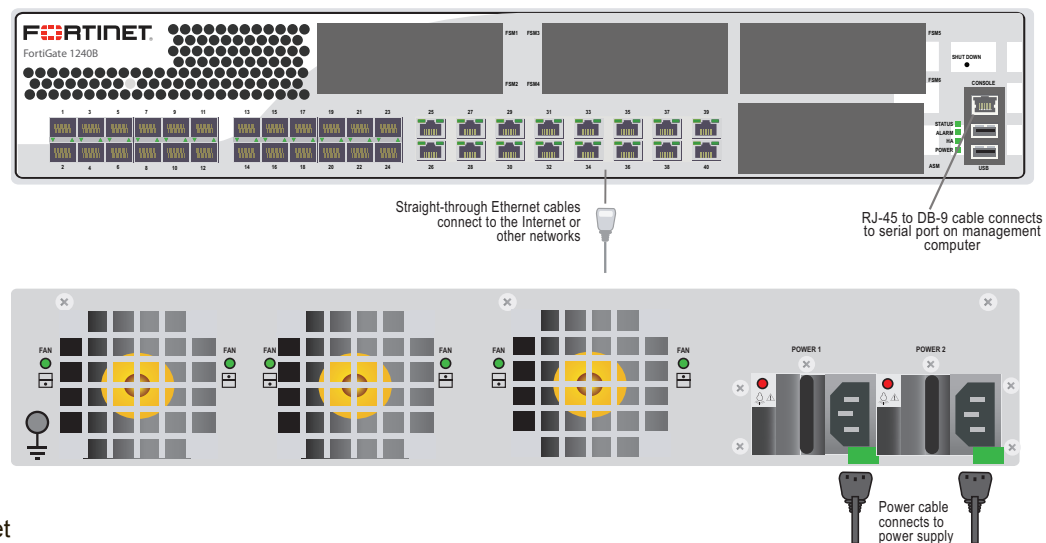
Connect the following to the FortiGate unit. Ensure the FortiGate unit is placed on a stable surface or install in a standard 19 inch rack.

- Connect the RJ-45 to DB-9 serial cable into the Console port on the unit. Insert the other end into the management computer.
- Insert the ethernet cable into a port. Insert the other end to the router connected to the Internet.
- Connect the AC power cable to the power supplies.
- Connect the AC power cords to a surge protected power bar or power supply.

**Caution:** Do not force the SFP transceivers into the cage slots. You can damage the connector if handling the SFP transceivers by holding the release Latch. If the transceiver does not easily slide in and click into place, it may not be aligned correctly or may be upside down. If this happens, remove the SFP transceiver, realign it or rotate it and slide it in again.

### To install the transceivers

1. Remove the caps from SFP cage sockets on the front panel.
2. Hold the sides of the SFP transceiver and slide the SFP transceiver into the cage socket until it clicks into place.



## FSM Modules

**Caution:** When installing the FSM module, ensure that the **FORTINET** and/or **"THIS SIDE UP"** labels are orientated upwards when inserting the module into the unit.

### To insert the FSM module

1. Insert the module into the FSM slot on the unit with the **Fortinet** and/or **"This Side Up"** labels facing upwards.
2. Close the latch.

Once you have installed the Fortinet solid state drive, you may need to format the hard disk drives using the CLI (if it has not been previously formatted).

### To format the SSD

- Type the following command in the CLI:  

```
exec formatlogdisk
```

# Collecting Information

## NAT/Route Mode

Port	IP:	_____
	Netmask:	_____
Port	IP:	_____
	Netmask:	_____
Port	IP:	_____
	Netmask:	_____
Port	IP:	_____
	Netmask:	_____
Port	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		Administrative account settings	
Port 1 interface	192.168.1.99	User name	admin
Port 2 interface	192.168.100.99	Password	(none)
Port 39 interface	192.168.2.99		
Port 40 interface	192.168.101.99		

To reset the FortiGate unit to the factory defaults, in the CLI type the command  
`execute factory reset`

# Configuration Tools

## Web Config

The FortiGate Web Config 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.
- A web browser such as FireFox or Internet Explorer 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 Tools and Documentation CD included with the FortiGate unit.

### Requirements:

- The RJ-45 to DB9 serial connection between the FortiGate unit and management computer.
- A terminal emulation application (HyperTerminal for Windows) on the management computer.

# Configuring

## NAT/Route mode

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.

## 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.

## Transparent mode

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.

## 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 internal
    set ip <intf_ip>/<netmask_ip>
  end
```
2. Repeat to configure each interface, for example, to configure the Port 1 interface.

```
config system interface
  edit port1
    ...
  end
```
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 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
```

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

Technical Documentation - <http://docs.forticare.com>  
Fortinet Knowledge Center - <http://kb.fortinet.com>  
Fortinet Technical Support - <http://support.fortinet.com>  
Training Services - <http://campus.training.fortinet.com>