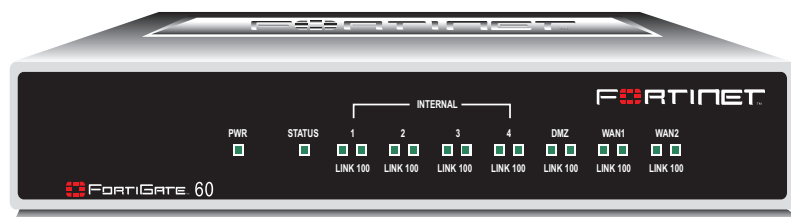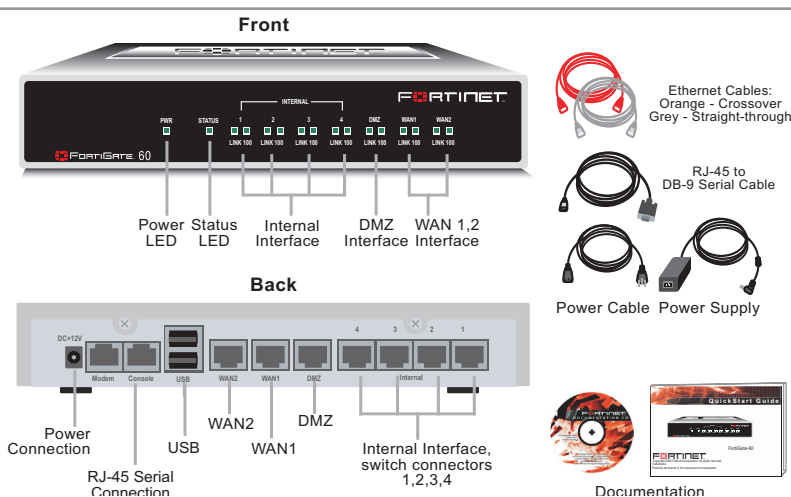| LED	State	Description
Power	Green	The FortiGate unit is on.
	Off	The FortiGate unit is off.
Status	Green/Flashing Green	The FortiGate unit is starting up.
	Off	The FortiGate unit is running normally.
Link (Internal, DMZ, WAN1, WAN2)	Green	The correct cable is in use and the connected equipment has power.
	Flashing Green	Network activity at this interface.
	Off	No link established.
100 (Internal, DMZ, WAN1, WAN2)	Green	The interface is connected at 100Mbps.

QuickStart Guide

FortiGate-60

FORTINET

™

1 Checking the Package Contents

Connector	Type	Speed	Protocol	Description
Internal	RJ-45	10/100 Base-T	Ethernet	A 4-port switch connection for up to four devices or the internal network.
WAN1 and WAN2	RJ-45	10/100 Base-T	Ethernet	Redundant connections to the Internet.
DMZ	RJ-45	10/100 Base-T	Ethernet	Optional connection to a DMZ network or to other FortiGate-60 units for high availability (HA). For details, see the Documentation CD-ROM.
Console	RJ-45	9600 Bps	RS-232	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB	USB		USB	Optional connection for the FortiUSB key, modem or backup operation.

Front

Power LED — Status LED — Internal Interface — DMZ Interface — WAN 1,2 Interface

Back

Power Connection — RJ-45 Serial Connection — USB — WAN2 — WAN1 — DMZ — Internal Interface, switch connectors 1,2,3,4

Ethernet Cables:
Orange - Crossover
Grey - Straight-through

RJ-45 to DB-9 Serial Cable

Power Cable   Power Supply

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. It requires 1.5 inches (3.75 cm) clearance above and on each side to allow for cooling.
- Plug in power cable to unit before connecting power.
- The Status light flashes while the unit is starting up and turns off when the system is up and running.

Power cable connects to power supply
Optional RJ-45 to DB-9 serial cable connects to management computer
Optional connection to a serial modem (serial to USB adapter required)
Optional redundant connection to Internet
Straight-through Ethernet cable connects to Internet (public switch, router or modem)
Optional connection to DMZ network
Straight-through Ethernet cables connect to computers on internal network

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 depends on the operating mode you select: NAT/Route mode (the default) or Transparent mode.

Quick configuration using the default settings

You can quickly set up your FortiGate unit for a home or small office using the web-based manager and the default settings in NAT/Route mode.
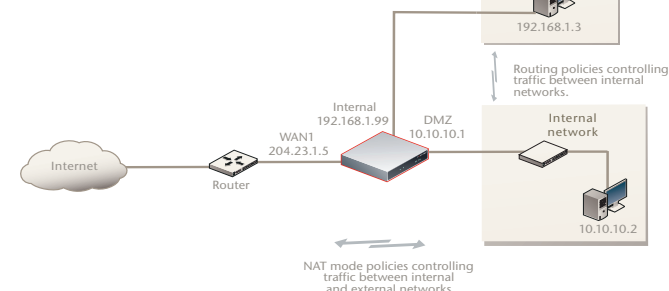All you need to do is set your network computers to use DHCP, access the web-based manager, and configure the required settings for the external interface. You can also configure DNS and a default route if needed. The FortiGate unit automatically assigns IP addresses for up to 100 computers in the internal network.
1. Connect the FortiGate unit to the network.
2. Set the all the network computers to use DHCP to automatically obtain an IP address. The FortiGate internal interface acts as a DHCP server for the internal network and assigns IP addresses to all computers in the range 192.168.1.110 –192.168.1.210.
3. From the management computer browse to https://192.168.1.99. The FortiGate web-based manager appears.
4. Go to **System** > **Network** > **Interface** and select Edit for the External interface.

5. Select one of the following Addressing modes
   - Manual: enter a static IP address and netmask, select OK, and go to step 6
   - DHCP: to get an IP address from the ISP select DHCP and go to step 9
   - PPPoE: to get an IP address from the ISP select PPPoE and go to step 9
6. Go to **System** > **Network** > **DNS**.
7. Select one of the following DNS settings
   - Obtain DNS server address automatically: select to get the DNS addresses from the ISP, select Apply
   - Use the following DNS server addresses: select and enter the DNS server addresses given to you by the ISP, select Apply
8. Go to **Router** > **Static**, select Create New, enter the default gateway address and select OK. Network configuration is complete. Proceed to part 7 of this *Quick Start Guide*.
9. Select Retrieve default gateway from server and Override internal DNS options if your ISP supports them, select OK, and proceed to part 7 of this *Quick Start Guide*.
Go to step 6 if you are not selecting these options.

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 that is connected to a network must be

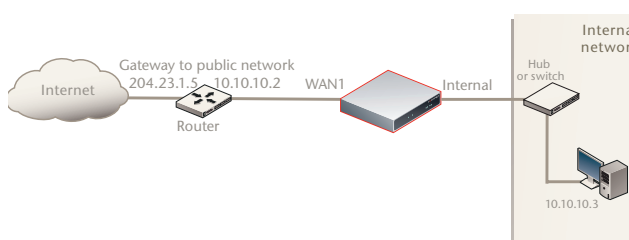configured with an IP address that is valid for that network.
You would typically use NAT/Route mode when the FortiGate unit is deployed as a gateway between private and public networks. In its default NAT/Route mode configuration, the unit functions as a firewall. Firewall policies control communications 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.

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.

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).

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 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

Internal Interface:	IP:	_____.____.____.____
	Netmask:	_____.____.____.____
WAN1 Interface:	IP:	_____.____.____.____
	Netmask:	_____.____.____.____
WAN2 Interface:	IP:	_____.____.____.____
	Netmask:	_____.____.____.____
DMZ	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 you will be managing the FortiGate unit from.

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
WAN1 interface	192.168.100.99	**Administrative account settings**	
WAN2 interface	192.168.101.99	User name	admin
DMZ interface	10.10.10.1	Password	(none)
DHCP server on the 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 > Status**, 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 in step 5 and select Apply.

Command Line Interface

1. Use the RJ-45 to DB-9 serial cable and converter 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: Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
3. At the Login: prompt, type admin and press Enter twice (no password required).

NAT/Rout mode

1. Configure the FortiGate internal interface.
```
config system interface
    edit internal
        set ip <intf_ip>/<netmask>
    end
```
2. Configure the FortiGate external interface.
```
config system interface
    edit wan1
        set ip <intf_ip>/<netmask>
```
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
```

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