



Hardware

FortiOS™ Handbook v3
for FortiOS 4.0 MR3



FortiOS™ Handbook: Hardware

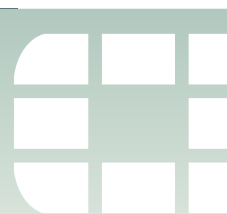
v3

23 July 2012

01-436-129361-20120723

for FortiOS 4.0 MR3

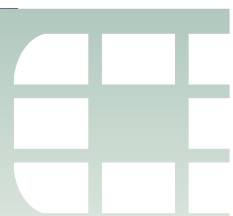
Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



Introduction	7
Before you begin	7
How this chapter is organized	7
FortiGate installation	9
Mounting the FortiGate unit	9
Desk or table mounting	9
Rack mounting	9
Rack mount considerations	9
Plugging in the FortiGate unit	17
Connecting to the network.	17
Turning off the FortiGate unit.	17
Further configuration	18
AMC module configuration	19
Configuring AMC modules	19
Auto-bypass and recovery for AMC bridge module	20
Enabling or disabling bypass mode for AMC bridge modules	21
FortiGate hardware accelerated processing	23
How hardware acceleration alters packet flow.	23
Network processors overview	25
Network processor models	25
Determining the network processors installed on your FortiGate unit.	26
Content processors overview	26
Determining the content processor in your FortiGate unit.	28
Security processing modules overview	28
Security processor module models	29
Displaying information about security processing modules	29
Example	29
Setting switch-mode mapping on the ADM-XD4	29
Configuring overall security priorities.	30
Configuring traffic offloading	30
Session fast path requirements	30
Packet fast path requirements	31
Fast path connections for specific FortiGate models	31
FortiGate-3040B	32
FortiGate-3140B	32
FortiGate-3140B — load balance mode.	33

FortiGate-3240C	34
FortiGate-3950B and FortiGate-3951B	35
Session offloading in HA active-active configuration	37
Configuring traffic shaping offloading	38
Example	39
Checking that traffic is offloaded	39
Disabling offloading	39
Multicast offloading / acceleration	40
Configuring IPsec VPN offloading	40
IPsec offloading requirements	40
Configuring HMAC check offloading.	41
Configuring VPN encryption/decryption offloading	41
Example	42
Examples of ASM-FB4 accelerated VPNs	42
Tunnel mode IPsec VPN example	43
Interface mode IPsec VPN example	44
Configuring IPS offloading	46
Configuring pre-IPS anomaly detection	46
Example	47
Configuring policy-based IPS on SP modules	47
Configuring interface-based IPS on SP modules	47
Examples	48
Accelerated tunnel mode IPsec	49
Accelerated interface mode IPsec	50
Configuring RAID	53
RAID levels	53
RAID-0	53
RAID-1	54
RAID-5	54
Configuring a RAID array	54
Checking the status of a RAID array	55
Rebuilding a RAID array	56
Why rebuild a RAID array?	56
How to rebuild the RAID array	56
FortiBridge installation and operation	59
Example FortiBridge application	59
Connecting the FortiBridge unit	60
Connecting the FortiBridge-2002 (copper gigabit ethernet).	61
Connecting the FortiBridge-2002F (fiber gigabit ethernet)	61

Normal mode operation	62
How the FortiBridge unit monitors the FortiGate unit	62
Probes and FortiGate firewall policies	63
Enabling probes to detect FortiGate hardware failure	65
Enabling probes to detect FortiGate software failure	65
Probe interval and probe threshold	65
Bypass mode operation	65
FortiBridge power failure	66
Example FortiGate HA cluster FortiBridge application	67
Connecting the FortiBridge-2002 (copper gigabit ethernet)	68
Connecting the FortiBridge-2002F (fiber gigabit ethernet).	68
Example configuration with other FortiGate interfaces.	68
Completing the basic FortiBridge configuration	71
Adding an administrator password	71
Changing the management IP address	71
Changing DNS server IP addresses	72
Changing the default gateway and adding static routes.	72
Allowing management access to the EXT1 interface	73
Changing the system time and date	73
Adding administrator accounts	73
Resetting to the factory default configuration	74
Installing FortiBridge unit firmware	74
Changing firmware versions	74
Installing firmware from a system reboot	75
Example network configuration	79
Configuring FortiBridge probes	80
Probe settings	81
To configure probe settings	81
Enabling probes	82
Verifying that probes are functioning.	84
Tuning the failure threshold and probe interval	84
Configuring FortiBridge alerts	84
FortiBridge alert email	85
FortiBridge syslog	85
FortiBridge SNMP	86
Recovering from a FortiGate failure	87
Manually switching between FortiBridge operating modes	88
Backing up and restoring the FortiBridge configuration	88
Appendix	91
Index	97



Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

FortiOS Handbook: Hardware describes how to install your FortiGate unit as well as some other hardware topics including the FortiBridge unit, hardware acceleration, and RAID.

This section contains the following topics:

- [Before you begin](#)
- [How this chapter is organized](#)

Before you begin

Before you begin using this guide, take a moment to note the following:

- Administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.
- Firewall policies limit access, and, while this and other similar features are a vital part of securing your network, they are not covered in this guide.
- If your FortiGate unit supports SSL acceleration, it also supports SSL content scanning and inspection for HTTPS, IMAPS, POP3S, and SMTPS traffic.

How this chapter is organized

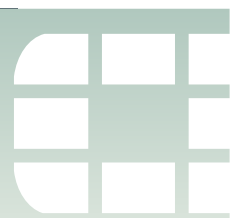
This FortiOS Handbook chapter contains the following sections:

[FortiGate installation](#) describes installing your FortiGate unit, and how to mount the FortiGate in a rack, if applicable.

[FortiGate hardware accelerated processing](#) some FortiGate models incorporate network processors in the main unit, others support the addition of AMC (Advanced Mezzanine Card) modules. The FortiGate-5000 series supports rear transition modules (RTMs) that incorporate network processors. This chapter describes how hardware acceleration works as well as how to take full advantage of its benefits.

[Configuring RAID](#) some FortiGate models have two or more hard disks configured in a RAID array to store log messages locally on the FortiGate unit. A RAID array can provide faster disk access, redundancy in case of partial failure, or both depending on the RAID level you select. This section describes how to configure RAID on FortiGate units that support it.

[FortiBridge installation and operation](#) describes a typical transparent mode FortiGate network and how to add a FortiBridge unit to provide fail open protection. In addition, detailed information about how FortiBridge units operate, a description of how to add a FortiBridge unit to an HA cluster, and connecting a FortiBridge unit to other FortiGate interfaces is included.



FortiGate installation

This chapter describes installing your FortiGate unit, environmental specifications, and how to mount the FortiGate unit.

This chapter contains the following topics:

- [Mounting the FortiGate unit](#)
- [Plugging in the FortiGate unit](#)
- [Turning off the FortiGate unit](#)
- [Further configuration](#)

Mounting the FortiGate unit

Most FortiGate units can be either rack mounted, or placed on a desk or table. Only the smallest units have no rack mounting hardware. The largest units are designed for rack mounting.

Desk or table mounting

Attach the provided rubber feet to the bottom of the FortiGate unit if they are not already attached.

Place the FortiGate unit on any flat, stable surface, ensure the unit has at least 1.5 inches (3.75 cm) of clearance on each side to ensure adequate airflow for cooling.

Rack mounting

If you are placing a 1U or 2U FortiGate unit into a rack, remove the rubber feet from the bottom of the FortiGate unit.

For rack mounting, use the mounting brackets and screws included with the FortiGate unit. The 3U 3900-series FortiGate units can be rack-mounted using either slide rails or middle-mount brackets and both procedures are covered below.

Rack mount considerations

Elevated operating ambient — If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.

Reduced air flow — Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical loading — Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

Circuit overloading — Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable ground — Reliable electrical grounding of rack-mounted equipment should be maintained.

Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).



Depending on the size of your FortiGate unit, you may require two or more people to safely install the unit in the rack.

To install a 1U or 2U FortiGate unit into a rack

- 1 Attach the mounting brackets to the side to the unit so that the brackets are on the front portion of the FortiGate unit. Ensure that the screws are tight.

The following photos illustrate how the brackets should be mounted. Note that the screw configuration may vary depending on your FortiGate unit.

Figure 1: Installed 1U mounting brackets



Figure 2: Installed 2U mounting brackets

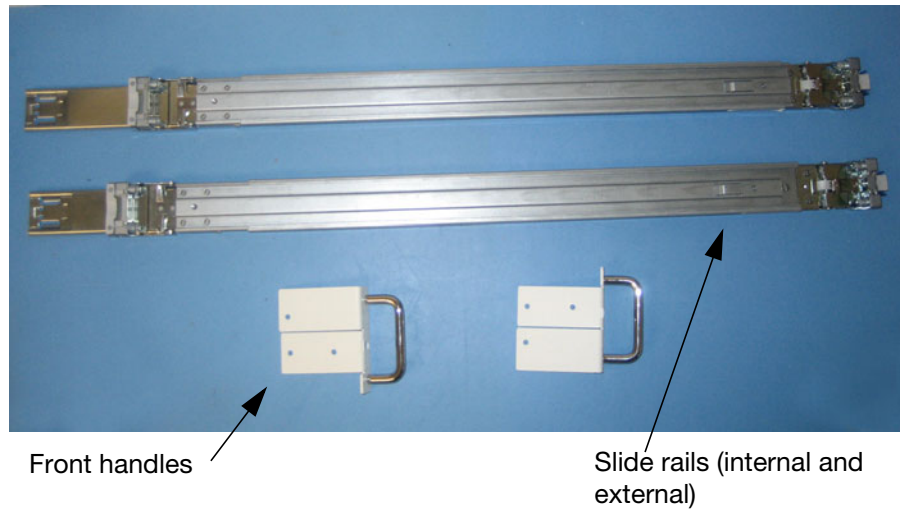


- 2 Position the FortiGate unit in the rack to allow for sufficient air flow.
- 3 Line up the mounting bracket holes to the holes on the rack, ensuring the FortiGate unit is level.
- 4 Finger tighten the screws to attach the FortiGate unit to the rack.
- 5 Once you verify the spacing of the FortiGate unit and that it is level, tighten the screws with a screwdriver. Ensure that the screws are tight.

The following photos illustrate how the mounting brackets and FortiGate unit should be attached to the rack.

Figure 3: Mounting a 1U FortiGate unit in a rack**Figure 4: Mounting a 2U FortiGate unit in a rack****To install a 3U 3900-series FortiGate using slide rails**

- 1 Before you start, confirm that you have the two slide rails and two front handles.

Figure 5: Slide rails and front handles.

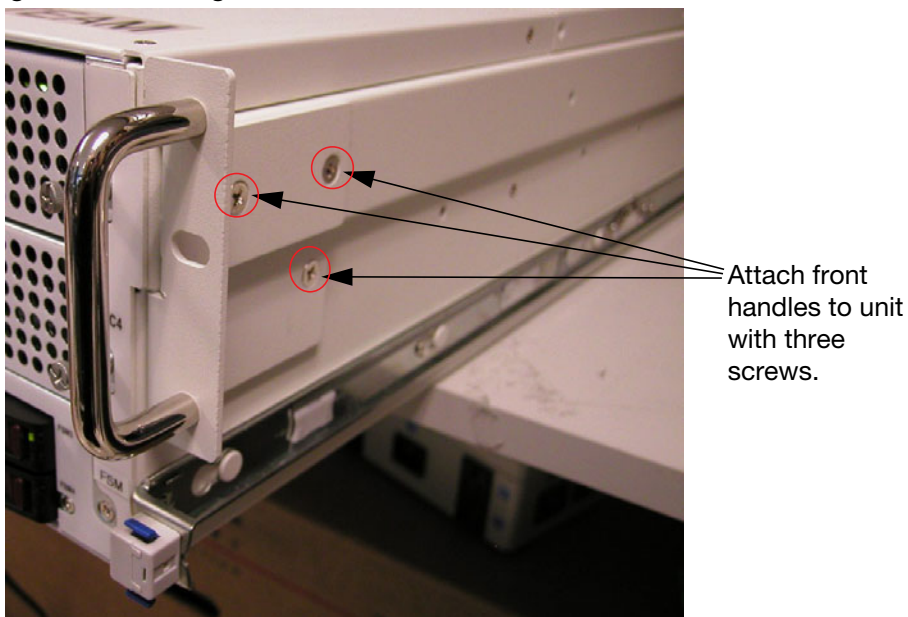
- 2 Attach the internal rails to each side of the unit. The rail should snap on and slide over until you hear a click from the rear clip.

Figure 6: Locking rear clip on unit.

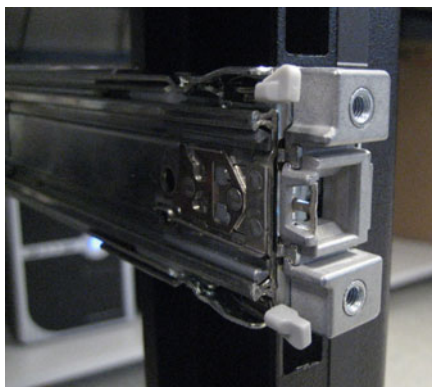
- 3 Optionally, you can add a screw to make the rail more secure.

Figure 7: Optional screw hole for additional support.

- 4 Attach the front handles to each side at the front of the unit with three screws. Note that the front handles are not used as rack mounts. Use only as handles to slide the unit in and out of the rack.

Figure 8: Attaching front handle to unit.

- 5 Orient the external rail on the rack. Ensure that the ball bearing track is forward. The front of the rail is labelled "Front" and the end of the rail is labelled "Rear".
- 6 Extend the external rail to fit the rack. Use the locking mechanism on the front and back of the rail to lock into place.

Figure 9: Front locking mechanism.**Figure 10: Rear locking mechanism.**

- 7 Use at least two people to lift the unit and insert the system approximately halfway onto the rack by sliding the external rails over the internal rails.
- 8 Slide the release tabs on both sides of the internal rails and push the system into the rack. Move your fingers away from the release tabs once the system is in motion.

Figure 11: FortiGate unit halfway on rack showing release tabs.

External rail
on rack

Internal rail on
unit

Slide release tabs forward and
push unit into rack

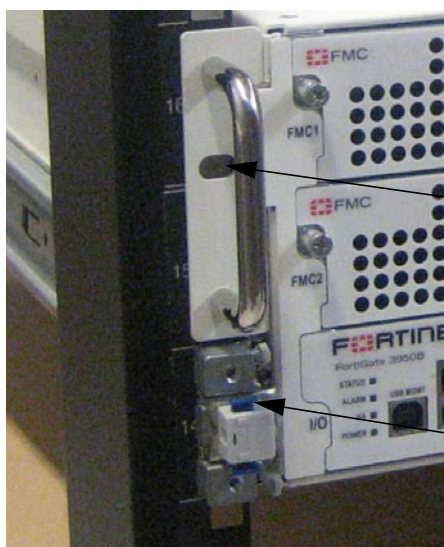
Use front
handles to
slide unit in
and out of
rack

- 9 Lock the system into place by squeezing together the buttons at the front of the rail.

Figure 12: FortiGate unit on rack.

Squeeze buttons to lock unit into place

10 Optionally, you can add a screw through the front handles for more security.

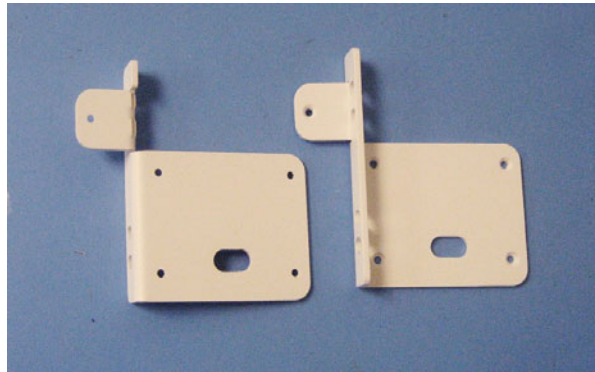
Figure 13: Location of locking mechanism on rail and screw hole in front handle.

Hole in front handle allows you to screw the unit to the rack

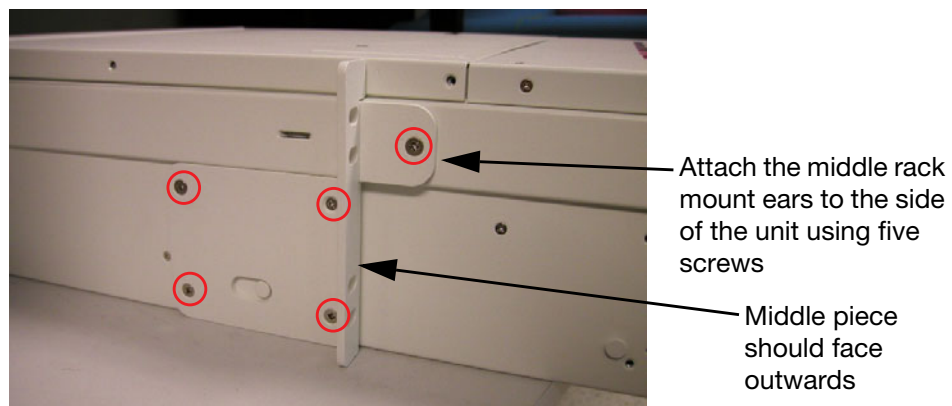
Locking mechanism on the rail.

To install a 3U 3900-series FortiGate using the middle rack mount brackets

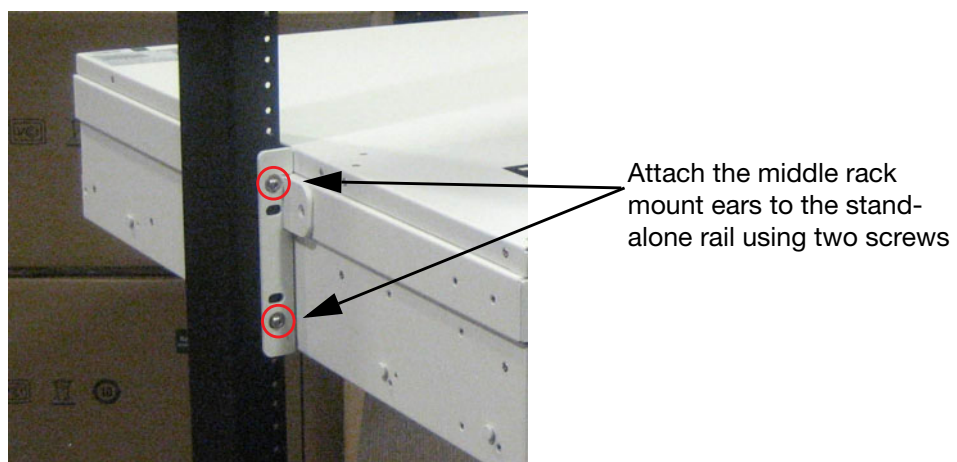
1 Before you start, confirm that you have the two middle rack mount brackets.

Figure 14: Middle rack mount brackets.

- 2 Attach the middle rack mount brackets to each side of the unit using five screws for each mount. Ensure the middle piece faces outwards.

Figure 15: Attaching the middle rack mount brackets to the sides of the unit.

- 3 Use at least two people to lift the unit and insert the system halfway onto the rack until the middle rack mount brackets meet the stand-alone rack.
- 4 While the two people hold the unit, use another person to attach the middle piece of the middle rack mount brackets to the stand-alone rack using two screws.

Figure 16: Attaching the middle rack mount brackets to the stand-alone rack.

- 5 Ensure you attach both middle rack mount brackets to both sides of stand-alone rack.

Figure 17: Fortinet unit on the stand-alone rack.



Plugging in the FortiGate unit

Most FortiGate units do not have an on/off switch. Check the quick-start guide included with your FortiGate unit to see if your model has an on/off switch.

To power on the FortiGate unit

- 1 Connect the power cable to the power connection on the back of the FortiGate unit. If your model has multiple power connections, connect cables to all the connections.
- 2 Connect the power cable or cables to power outlets.

Each power cable should be connected to a different power source. If one power source fails, the other may still be operative.

The FortiGate unit starts and the Power and Status (if available) LEDs light up. The Status LED (if available) flashes while the FortiGate unit starts, and remains lit when the system is running.



If the FortiGate unit has two power supplies and only one is connected, an audible alarm sounds to indicate a failed power supply. Press the red alarm cancel button on the rear panel next to the power supply to stop the alarm.

Connecting to the network

Using the supplied Ethernet cable, connect one end of the cable to your router or modem, whichever is the connection to the Internet. Connect the other end to the FortiGate unit. Connect it to either the External, WAN port, or port 1 interface. Use additional cables to connect the Internal port or port 2 to your internal hub or switch.

Turning off the FortiGate unit

Always shut down the FortiGate operating system properly before turning off the power switch or unplugging the unit to avoid potential hardware problems.

To power off the FortiGate unit

- 1 From the web-based manager, go to *System > Dashboard > Status*.
- 2 In the *Unit Operation* display, select *Shutdown*, or from the CLI enter:
`execute shutdown`
- 3 Wait a moment for the shutdown operation to finish.
- 4 Disconnect the power cables from the power supply.

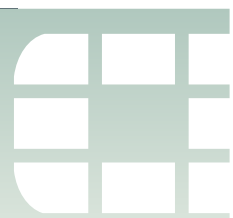
Further configuration

Further configuration is beyond the scope of this installation guide.

The [System Administration](#) document describes how to configure the operating mode, interface addresses, DNS server, and the default gateway.



Management interfaces do not support VLANs



AMC module configuration

This section explains how to configure AMC modules on the FortiGate unit. This includes auto-bypass and recovery for AMC bridge modules.

The following topics are included in this section:

- [Configuring AMC modules](#)
- [Auto-bypass and recovery for AMC bridge module](#)
- [Enabling or disabling bypass mode for AMC bridge modules](#)

Configuring AMC modules

By default, FortiGate units automatically recognize the AMC modules installed in their AMC slots or automatically recognize that an AMC slot is empty. If the module contains interfaces, FortiOS automatically adds the interfaces to the FortiGate configuration. If the module contains a hard disk, the hard disk is automatically added to the configuration. However, when the FortiGate unit is powered down and the module removed from the slot, when the FortiGate unit restarts it automatically recognizes that the slot is empty and will not retain any configuration settings for the missing module.

This default behavior is usually acceptable in most cases. However, it can be useful when a module is present in a slot to add the name of the module to the FortiGate configuration. Then, if the module fails or if you temporarily remove it from the slot, the FortiGate unit keeps the module's configuration settings so that when the module is replaced you will not have to re-configure it.

If you have added the name of a module to a slot and you are planning or removing the module and replacing it with a different type of module (for example, if you are removing a FortiGate-ASM-S08 and replacing it with a FortiGate-ASM-FX2) you should reset the slot to the default before removing the module. Then after adding the new module you should add its name to the slot.

You configure AMC slot settings from the FortiGate CLI using the `config system amc` command. For information about this command, see the [FortiGate CLI Reference](#).

The following procedure shows how to add a FortiGate-ADM-FB8 to the first double-width AMC slot (dw1) and how to add the name of the module to the slot configuration.

To change the default setting for an AMC slot

- 1 Enter the following CLI command to verify that the slot that you will insert the FortiGate-ADM-FB8 module into is set to the default configuration.

This command lists the AMC slots and the settings for each one. Example command output for a FortiGate-5001A with an empty double-width AMC slot:

```
get system amc
dw1          : auto
```

- 2 Power down the FortiGate unit.
- 3 Insert the FortiGate-ADM-FB8 module into the double-width AMC slot.

- 4 Power up the FortiGate unit.

As long as the slot that you have inserted the FortiGate-ADM-FB8 module into is set to `auto` the FortiGate unit should automatically find the module when it powers up.

- 5 Add the name of the FortiGate-ADM-FB8 module to the FortiGate configuration.

```
config system amc
    set dw1 adm-fb8
end
```

Auto-bypass and recovery for AMC bridge module

The FortiGate-ASM-CX4 and FortiGate-ASM-FX2 modules provide fail open protection for interface pairs of FortiGate units operating in Transparent mode and that have a single-width AMC slot. The FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module bridges FortiGate interfaces, monitors the interfaces for traffic failures, and operate as pass-through devices if the interfaces or the entire FortiGate unit fails or for some reason cannot pass traffic between the interfaces. If a failure occurs, traffic bypasses the FortiGate unit and passes through the FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module to make sure that the network can continue processing traffic after a FortiGate failure.

This section describes how to configure a FortiGate unit to use a FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module to bridge FortiGate interfaces. The FortiGate unit must operate in Transparent mode and the FortiGate-ASM-CX4 and FortiGate-ASM-FX2 modules are not compatible with FortiGate HA.

The FortiGate-ASM-CX4 and FortiGate-ASM-FX2 modules include a bypass watchdog that continually verifies that traffic is flowing through the bridged FortiGate interfaces. If traffic stops flowing, for example if the FortiGate unit fails, and if the bypass watchdog detects this, the bridge module switches to bypass mode to ensure the flow of traffic on the network.

In bypass mode all traffic flows between interfaces on the FortiGate-ASM-CX4 and FortiGate-ASM-FX2 modules and not through the FortiGate unit. You can configure a recovery watchdog to verify that the bridged FortiGate interfaces cannot process traffic. If you fix the problem or the problem fixes itself, the recovery watchdog automatically detects that traffic can resume and switches the module back to normal operation by turning off bypass mode.

To configure a FortiGate unit to operate with a FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module

- 1 Switch the FortiGate unit to operate in transparent mode.

```
config system settings
    set opmode transparent
    set manageip <management_IPv4> <netmask_ipv4>
    set gateway <gateway_ipv4>
end
```

After a short pause the FortiGate unit is operating in transparent mode.

- 2 Enter the following command to verify that the slot that you will insert the FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module into is set to `auto`.

This command lists the AMC slots and the settings for each one. Example command output for a FortiGate-620B with an empty AMC slot:

```
get system amc
sw1          : auto
```

- 3 Power down the FortiGate unit.
- 4 Insert the FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module into a single-width AMC slot.
- 5 Power up the FortiGate unit.

As long as the slot that you have inserted the module into is set to `auto` the FortiGate unit should automatically find the module when it powers up.

- 6 Add the name of the module to the FortiGate configuration and configure bypass and recovery settings.

The following command configures AMC single width slot 1 (sw1) for a FortiGate-ASM-CX4.

This command also enables the bypass watchdog and increases the bypass timeout from the default value of 10 seconds to 60 seconds. This means that if a failure occurs the bridge module will change to bypass mode 60 seconds after the bypass watchdog detects the failure.

This command also enables watchdog recovery and sets the watchdog recovery period to 30 seconds. This means that if a failure occurs, while the FortiGate-ASM-CX4 module is bridging the connection the AMC bypass watchdog monitors FortiGate processes and will revert to normal operating mode (that is disable the bridging the interfaces with the FortiGate-ASM-CX4 module) if the FortiGate unit recovers from the failure.

```
config system amc
  set sw1 asm-cx4
  set bypass-watchdog enable
  set bypass-timeout 60
  set watchdog-recovery enable
  set watchdog-recovery-period 30
end
```

Enabling or disabling bypass mode for AMC bridge modules

Use the `execute amc bypass` command to switch between normal mode and bypass mode for a FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module installed in a single-width AMC slot in a FortiGate unit. Normally the FortiGate-ASM-CX4 and FortiGate-ASM-FX2 modules operate with bypass mode disabled and traffic passes through the FortiGate interfaces bridged by the FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module. You can use this command manually enable bypass mode and force traffic to bypass the FortiGate interfaces and pass through the FortiGate-ASM-CX4 or FortiGate-ASM-FX2 module.

Also, if bypass mode has been enabled (using this command or because of a failure), you can also use this command to manually disable bypass mode and resume normal operation. This can be useful if the problem that caused the failure has been fixed and normal operation can resume.

To manually enable bypass mode

- 1 Use the following command to manually enable bypass mode:
`execute amc bypass enable`

- 2 Use the following diagnose command to view the status of the AMC modules installed in a FortiGate unit, including whether they are operating in bypass mode.

For example if you have installed a FortiGate-ASM-CX4 module in AMC slot 2 of a FortiGate-3810A and bypass mode is enabled:

```
diagnose sys amc bypass status
ASM-CX4 in slot 2:
    amc-sw2/1 <--> amc-sw2/2: mode=bypass (admin action)
    amc-sw2/3 <--> amc-sw2/4: mode=bypass (admin action)
```

```
Daemon heartbeat status: normal
Last heartbeat received: 0 second(s) ago
```

- 3 Log into the web-based manager and go to *System > Dashboard > Status* and view the *Unit Operation* widget to see the status of the AMC bridge module.

To manually disable bypass mode

- 1 Use the following command to manually disable bypass mode:

```
execute amc bypass disable
```

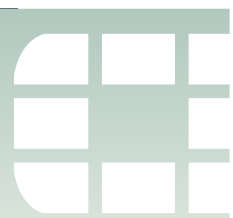
- 2 Use the following diagnose command to view the status of the AMC modules installed in a FortiGate unit, including whether they are operating in bypass mode.

For example if you have installed a FortiGate-ASM-CX4 module in AMC slot 2 of a FortiGate-3810A and bypass mode is disabled:

```
diagnose sys amc bypass status
ASM-CX4 in slot 2:
    amc-sw2/1 <--> amc-sw2/2: mode=normal
    amc-sw2/3 <--> amc-sw2/4: mode=normal
```

```
Daemon heartbeat status: normal
Last heartbeat received: 1 second(s) ago
```

- 3 Log into the web-based manager and go to *System > Dashboard > Status* and view the *Unit Operation* widget to see the status of the AMC bridge module.



FortiGate hardware accelerated processing

Many FortiGate models can offload some types of network traffic processing from main processing resources to specialized network processors. If your network has a significant volume of traffic that is suitable for offloading, this hardware acceleration can significantly improve your network throughput.

Some FortiGate models incorporate network processors in the main unit, others support the addition of AMC (Advanced Mezzanine Card) modules. The FortiGate-5000 series supports rear transition modules (RTMs) that incorporate network processors.

This chapter contains the following topics:

- [How hardware acceleration alters packet flow](#)
- [Network processors overview](#)
- [Content processors overview](#)
- [Security processing modules overview](#)
- [Configuring overall security priorities](#)
- [Configuring traffic offloading](#)
- [Configuring IPsec VPN offloading](#)
- [Configuring IPS offloading](#)

How hardware acceleration alters packet flow

Hardware acceleration generally alters packet processing flow as follows:

- 1 Packets initiating a session pass to the FortiGate unit's main processing resources.
- 2 The FortiGate unit assesses whether the session matches fast path (offload) requirements.

To be suitable for offloading, traffic must possess only characteristics that can be processed by the fast path. For a list of requirements, see [“Configuring traffic offloading” on page 30](#).

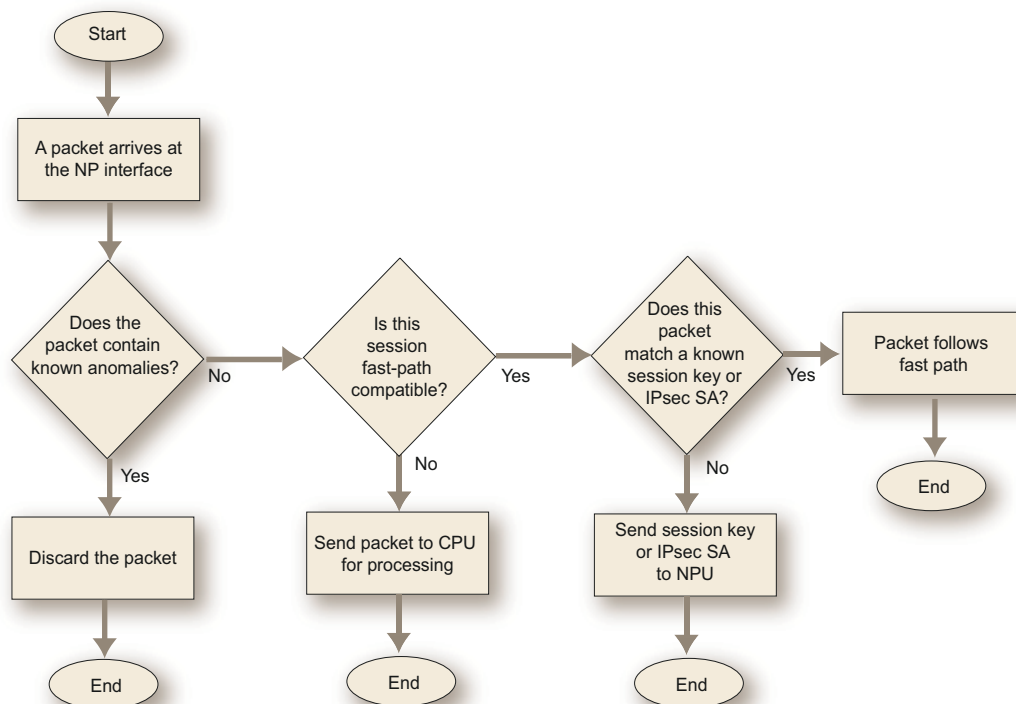
If the traffic is categorized as fast path friendly, the FortiGate unit sends the session key or IPsec security association (SA) and configured processing action to the network processor(s).

- 3 Network processors continuously match packets arriving on their attached ports against the session keys and SAs they have received from the FortiGate unit's main processing resources.
- If a network processor's network interface is configured to perform hardware accelerated anomaly checks, the network processor drops or accepts packets which match the configured anomaly patterns. These checks are separate from and in advance of anomaly checks performed by IPS, which is not compatible with network processor offloading. See [“Configuring pre-IPS anomaly detection” on page 46](#).
 - The network processor next checks for a matching session key or SA. If a matching session key or SA is found, and if the packet meets packet requirements, the network processor processes the packet according to the configured action and then sends the resulting packet. Packet processing is hardware accelerated.
 - If a matching session key or SA is not found, or if the packet does not meet packet requirements, the traffic cannot be offloaded. The network processor sends the data to the FortiGate unit's main processing resources, which process the packet. Packet processing is similar to normal network interfaces (that is, packet processing is not hardware accelerated by the network processor, and requires main processing resources). Packet forwarding occurs at normal rates.



Network processors do not count offloaded packets, and offloaded packets will not be included in traffic statistics, such as FortiAnalyzer traffic reports.

Figure 18: Deciding the packet flow for accelerated interfaces



Some traffic processing can still be hardware accelerated, even though it does not meet general offloading requirements. For example, some IPsec traffic originates from the FortiGate unit itself and does not follow the offloading requirement of ingress from a network processor's network interface, but FortiGate units can still utilize network processor encryption capabilities. See [“Configuring IPsec VPN offloading” on page 40](#).

Packet forwarding rates vary by the percentage of offloadable processing and the type of network processing required by your configuration, but are independent of frame size. For optimal traffic types, network throughput can equal wire speed.

Offloading requirements vary slightly by the model of the network processor.

The following types of acceleration hardware are found on FortiGate units:

- network processors: NP1 (formerly known as FA2), NP2, NP4
- content processors: CP4, CP5, CP6
- accelerated interface modules: ASM-FB4, ADM-FB8, ADM-XB2, ADM-XD4, RTM-XD2
- security processor modules: ASM-CE4, ASM-XE2

Network processors overview

Many Fortinet products contain network processors. Some of these products contain NP1 network processors (also known as FortiAccel, or FA2), while others contain NP2 network processors. Some newer models contain an NP4 processor. Network processor features, and therefore offloading requirements, vary by network processor model. Differing offloading requirements are noted in [“Configuring traffic offloading” on page 30](#) and [“Configuring IPsec VPN offloading” on page 40](#).

Network processor models

FortiASIC network processors work at the interface level to support IPsec offload and unicast UDP/TCP traffic forwarding. The maximum throughput and number of network interfaces varies by processor model.

NP1: supports FW and VPN acceleration with 2Gbps capacity. It is found on FortiGate units such models 1000A-FA2, 3600A, and 3810A, and also on FortiGate-5000 series 5001FA2 and 5005FA2 blades.

NP2: supports FW and VPN acceleration with 4Gbps capacity. It is found on newer, B-series FortiGate units ranging from models 200B to 3016B, and on most AMC accelerated interface cards.

NP4: supports FW and VPN acceleration with 40 Gbps capacity. It is found on the ADM-XD4 AMC card and on the FortiGate-5000 series RTM-XD2 blade.

Table 1: Network processor models

Processor	Interfaces
NP1	2 x 1 Gb/s
NP2	1 x 10Gb/s, 4 x 1Gb/s
NP4	2 x 10Gb/s



The NP1 network processor does not support frames greater than 1500 bytes. If your network uses jumbo frames, you may need to adjust the MTU (Maximum Transmission Unit) of devices connected to NP1 ports. Maximum frame size for NP2 and NP4 processors is 9000 bytes.



For both NP1 and NP2 network processors, ports attached to a network processor cannot be used for firmware installation by TFTP.

Some Fortinet products contain multiple network processors. Depending on the product, network processors may or may not be directly connected to each other on the circuit board through an EEI (Enhanced Extension Interface).

- Directly connected network processors have an EEI, and can pass traffic between them without involving the FortiGate unit's main processing resources.
- Indirectly connected network processors have no EEI, and **cannot** pass traffic between them without involving the FortiGate unit's main processing resources.

Sessions can only be offloaded if both the source and destination port are connected to the same network processor or directly (EEI) connected network processor pair.

For information about the network processors in any specific FortiGate model, refer to the product brochure.

Determining the network processors installed on your FortiGate unit

To list the network processors on your FortiGate unit, use the following CLI command.

```
get hardware npu <model> list
```

<model> can be np1, np2 or np4.

The output lists the interfaces that have the specified processor. For example,

```
# get hardware npu np1 list
ID      Interface
0       port9 port10
```

This command does not detect Security processing modules.

Content processors overview

The FortiASIC Content Processor (CP) works at the system level. Its main functions are SSL VPN key generation and SSL offloading. Capabilities vary by model.

CP4

- FIPS-compliant DES/3DES/AES encryption and decryption

- SHA-1 and MD5 HMAC
- IPSEC protocol processor
- Random Number generator
- Public Key Crypto Engine
- Content processing engine
- ANSI X9.31 and PKCS#1 certificate support

CP5

- FIPS-compliant DES/3DES/AES encryption and decryption
- SHA-1 and MD5 HMAC with RFC1321/2104/2403/2404 and FIPS180/FIPS198
- IPsec protocol processor
- High performance IPSEC Engine
- Random Number generator compliant with ANSI X9.31
- Public Key Crypto Engine supports high performance IKE and RSA computation
- Script Processor

CP6

- Dual content processors
- FIPS-compliant DES/3DES/AES encryption and decryption
- SHA-1 and MD5 HMAC with RFC1321 and FIPS180
- HMAC in accordance with RFC2104/2403/2404 and FIPS198
- IPsec protocol processor
- High performance IPsec engine
- Random Number generator compliance with ANSI X9.31
- Key exchange processor for high performance IKE and RSA computation
- Script Processor
- SSL/TLS protocol processor for SSL content scanning and SSL acceleration

CP8

- Over 10Gbps throughput IPS content processor for packet content matching with signatures
- High performance VPN bulk data engine
 - IPSEC and SSL/TLS protocol processor
 - DES/3DES/AES in accordance with FIPS46-3/FIPS81/FIPS197
 - ARC4 in compliance with RC4
 - MD5/SHA-1/SHA256 with RFC1321 and FIPS180
 - HMAC in accordance with RFC2104/2403/2404 and FIPS198

- Key Exchange Processor support high performance IKE and RSA computation
 - Public key exponentiation engine with hardware CRT support
 - Primarily checking for RSA key generation
 - Handshake accelerator with automatic key material generation
 - Random Number generator compliance with ANSI X9.31
 - Sub public key engine (PKCE) to support up to 4094 bit operation directly
- Message authentication module offers high performance cryptographic engine for calculating SHA256/SHA1/MD5 of data up to 4G bytes (used by any application like WAN opt.)
- PCI express Gen 2 four lanes interface
- Cascade Interface for chip expansion

Determining the content processor in your FortiGate unit

Use the `get hardware status` CLI command to determine which content processor your FortiGate unit contains. The output looks like this:

```
# get hardware status
Model name: Fortigate-620B
ASIC version: CP6
ASIC SRAM: 64M
CPU: Intel(R) Core(TM)2 Duo CPU      E4300   @ 1.80GHz
RAM: 2020 MB
Compact Flash: 493 MB /dev/sda
Hard disk: 76618 MB /dev/sdb
USB Flash: not available
Network Card chipset: Broadcom 570x Tigon3 Ethernet Adapter
(rev.0x5784100)
```

The ASIC version line lists the content processor model number.

If you have a CP6 processor, you can view the status of SSL acceleration using the command `get vpn status ssl hardware-acceleration`.

Security processing modules overview

FortiGate Security Processing (SP) modules, such as the ASM-CE4 and ADM-XE2, work at both the interface and system level to increase overall system performance by accelerating some security and networking processing on the interfaces they provide. The SP frees the FortiGate unit's processor for other tasks by offloading firewall, application control, and IPS processing, including flow-based antivirus protection. You can configure the SP to favor IPS over firewall processing in hostile high-traffic environments.

The ASM-CE4 and ADM-XE2 are Advanced Mezzanine cards (AMCs) that are the first generation of SP modules. The next generation of SP modules are Fortinet Mezzanine cards (FMCs) found on newer FortiGate models, such as the 3950. FMC modules take advantage of the Integrated Switch Fabric (ISF) backplane, meaning that accelerated performance is available between any two interfaces, not just interfaces on the same FMC module.

Security processor module models

The ADM-XE2 is a dual-width AMC module with two 10 Gb/s interfaces that can be used on FortiGate-3810A and FortiGate-5001A-DW systems.

The ADM-FE8 is a dual-width AMC module with eight 1 Gb/s interfaces that can be used with the FortiGate-3810A.

The ASM-CE4 is a single-width AMC module with four 10/100/1000 Mb/s interfaces that can be used on FortiGate-3016B and FortiGate-3810A units.

The FMC-XG2 is an FMC module with two 10 Gb/s SPF+ interfaces that can be used on FortiGate-3950B and FortiGate-3951B units. The FortiGate-3140B also contains a built-in FMC-XG2 using ports 19 and 20.

Displaying information about security processing modules

You can display information about installed AMC modules using the CLI command

```
diagnose npu spm dos synproxy <sp_id>
```

Variable	Description
<sp_id>	Enter the ID of the security processing device that you want to display information for. The first device is 0, the second is 1, and so on.



Security processing modules are also called network processing units (NPUs).

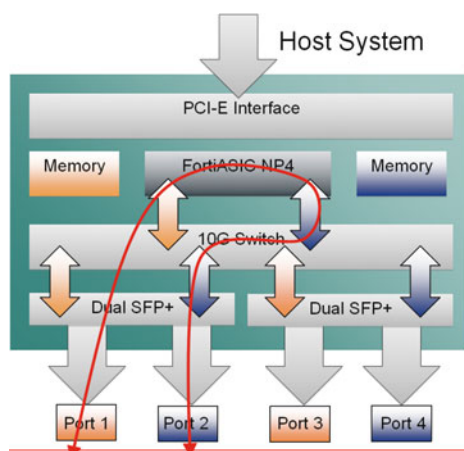
Example

This example shows how to display details about how the module is processing sessions using the syn proxy. This is a partial output of the command:

```
Number of proxied TCP connections : 0
Number of working proxied TCP connections : 0
Number of retired TCP connections : 0
Number of valid TCP connections : 0
Number of attacks, no ACK from client : 0
Number of no SYN-ACK from server : 0
Number of reset by server (service not supported): 0
Number of established session timeout : 0
Client timeout setting : 3 Seconds
Server timeout setting : 3 Seconds
```

Setting switch-mode mapping on the ADM-XD4

The ADM-XD4 SP has four 10 Gb/s ports, but the NP4 processor it contains has only two 10 Gb/s ports. The external ports you use are important to optimize the SP for your application.

Figure 19: ADM-XD4 mapping mode

Ports 1 and 3 share one NP4 processor and ports 2 and 4 share the other. Performance ports sharing the same NP4 processor is far better than when forcing network data to move between NP4 processors by using one port from each, for example ports 1 and 2 or ports 3 and 4.

Configuring overall security priorities

You can set the priority for security processing using the CLI:

```
config system global
  set optimize {antivirus | throughput | session}
end
```

antivirus - Allow all CPU cores to process traffic – typically used with proxy style services (AntiX, content filtering)

throughput - Prevents code synchronisation delays from impacting raw throughput.

session - Allows distributed session set up across all cores for high session per second environments. This option is available on newer FortiGate models such as the 1240B.

Configuring traffic offloading

Offloading traffic to a network processor requires that the FortiGate unit configuration and the traffic itself is suited to hardware acceleration. There are requirements for path the sessions and the individual packets.

Session fast path requirements

Sessions must be fast path ready. Fast path ready session characteristics are:

- Layer 2 type/length must be 0x0800 (IEEE 802.1q VLAN specification is supported); link aggregation between any network interfaces sharing the same network processor(s) may be used (IEEE 802.3ad specification is supported)
- Layer 3 protocol must be IPv4
- Layer 4 protocol must be UDP, TCP or ICMP
- Layer 3 / Layer 4 header or content modification must not require a session helper (for example, SNAT, DNAT, and TTL reduction are supported, but application layer content modification is not supported)

- FortiGate unit firewall policy must not require antivirus or IPS inspection
- origin must not be local host (the FortiGate unit)
- ingress and egress network interfaces are both attached to the same network processor(s)



If you disable anomaly checks by Intrusion Prevention (IPS), you can still enable hardware accelerated anomaly checks using the `fp-anomaly` field of the `config system interface` CLI command. See “[Configuring pre-IPS anomaly detection](#)” on page 46.



For session offloading to NP1 network processors, the session must not use an aggregated link or require QoS, including rate limits and bandwidth guarantees. Traffic shaping and link aggregation are not supported.

If a session is not fast path ready, the FortiGate unit will not send the session key to the network processor(s). Without the session key, all session key lookup by a network processor for incoming packets of that session fails, causing all session packets to be sent to the FortiGate unit’s main processing resources, and processed at normal speeds.

If a session is fast path ready, the FortiGate unit will send the session key to the network processor(s). Session key lookup then succeeds for subsequent packets from the known session.

Packet fast path requirements

Packets within the session must then also meet packet requirements.

- Incoming packets must not be fragmented.
- Outgoing packets must not require fragmentation to a size less than 385 bytes. Because of this requirement, the configured MTU (Maximum Transmission Unit) for network processors’ network interfaces must also meet or exceed the network processors’ supported minimum MTU of 385 bytes.

If packet requirements are not met, an individual packet will use FortiGate unit main processing resources, regardless of whether other packets in the session are offloaded to the specialized network processor(s).

In some cases, due to these requirements, a protocol’s session(s) may receive a mixture of offloaded and non-offloaded processing.

For example, FTP uses two connections: a control connection and a data connection. The control connection requires a session helper, and cannot be offloaded, but the data connection does not require a session helper, and can be offloaded. Within the offloadable data session, fragmented packets will not be offloaded, but other packets will be offloaded.

Some traffic types differ from general offloading requirements, but still utilize some of the network processors’ encryption and other capabilities. Exceptions include IPsec traffic and active-active high availability (HA) load balanced traffic.

Fast path connections for specific FortiGate models

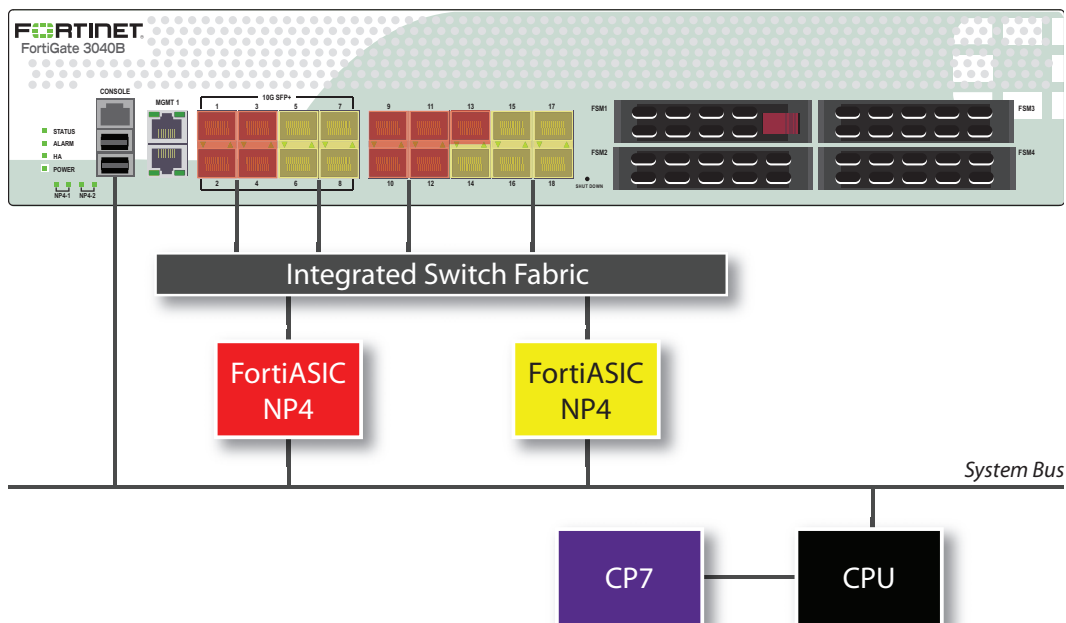
A number of FortiGate models contain multiple NP4 processors that require care when connecting network cables. For accelerated processing, traffic must enter and exit interfaces connected to the same NP4 processor.

FortiGate-3040B

The FortiGate-3040B features two NP4 processors to accelerate network traffic to wire speeds. Traffic between interfaces that use the same processor experience the highest acceleration.

- The 10 Gb interfaces, port1, port2, port3, port4, and the 1 Gb interfaces, port9, port10, port11, port12, port13, share connections to one NP4 processor.
- The 10 Gb interfaces, port5, port6, port7, port8, and the 1 Gb interfaces, port14, port15, port16, port17, port18, share connections to the other NP4 processor.

Figure 20: The FortiGate-3040B

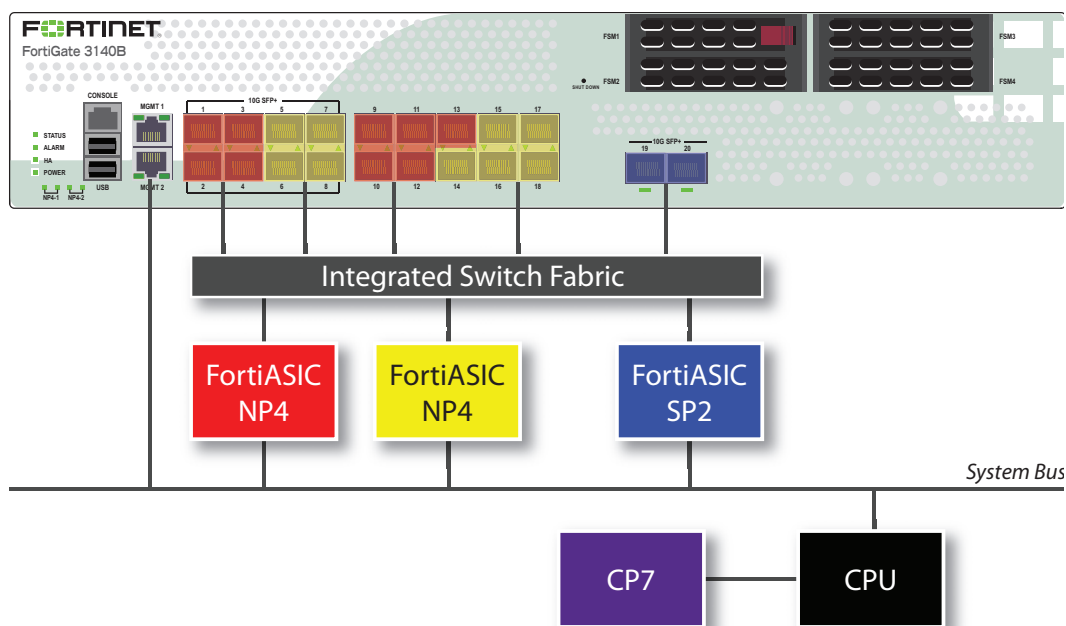


For example, for maximum NP4 acceleration of traffic received on port1, the traffic must exit the FortiGate-3040B unit on port2, port3, or port4 if the bandwidth exceeds 1 Gb. If the traffic bandwidth does not exceed 1 Gb, the traffic can also exit on port9, port10, port11, port12, or port13. Also, for maximum NP4 acceleration of traffic received on port5, the traffic must exit the FortiGate-3040B unit on port6, port7, or port8 if the bandwidth exceeds 1 Gb. If the traffic bandwidth does not exceed 1 Gb, the traffic can also exit on port14, port15, port16, port17, or port18.

FortiGate-3140B

The FortiGate-3140B features two NP4 processors and one SP2 processor to accelerate network traffic to wire speeds. Traffic between interfaces that use the same processor experience the highest acceleration.

- The 10 Gb interfaces, port1, port2, port3, port4, and the 1 Gb interfaces, port9, port10, port11, port12, port13, share connections to one NP4 processor.
- The 10 Gb interfaces, port5, port6, port7, port8, and the 1 Gb interfaces, port14, port15, port16, port17, port18, share connections to the other NP4 processor.
- The 10 Gb interfaces, port19 and port20, share connections to the SP2 processor.

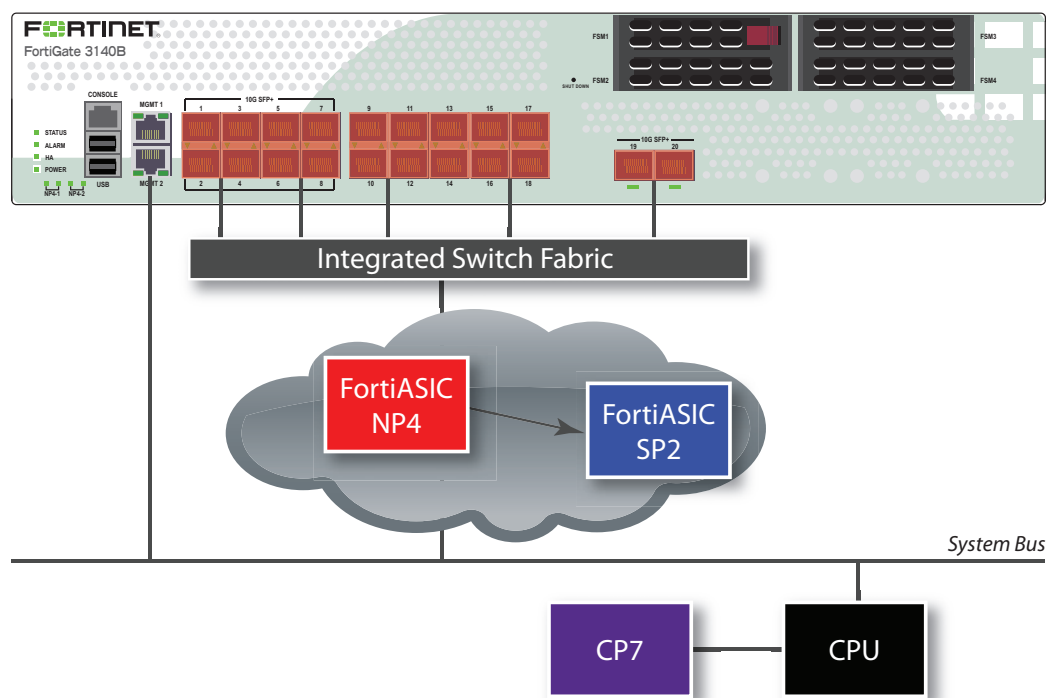
Figure 21: The FortiGate-3140B

For example, for maximum NP4 acceleration of traffic received on port1, the traffic must exit the FortiGate-3140B unit on port2, port3, or port4 if the bandwidth exceeds 1 Gb. If the traffic bandwidth does not exceed 1 Gb, the traffic can also exit on port9, port10, port11, port12, or port13. For maximum NP4 acceleration of traffic received on port5, the traffic must exit the FortiGate-3140B unit on port6, port7, or port8 if the bandwidth exceeds 1 Gb. If the traffic bandwidth does not exceed 1 Gb, the traffic can also exit on port14, port15, port16, port17, or port18. Also, for maximum SP2 acceleration of traffic received on port 19, the traffic must exit the FortiGate-3140B unit on port20.

FortiGate-3140B — load balance mode

The FortiGate-3140B load balance mode allows you increased flexibility in how you use the interfaces on the FortiGate unit. When enabled, traffic between any two interfaces (excluding management and console) is accelerated. Traffic is not limited to entering and leaving the FortiGate unit in specific interface groupings to benefit from NP4 and SP2 acceleration. You can use any pair of interfaces.

Security acceleration in this mode is limited, however. Only IPS scanning is accelerated in load balance mode.

Figure 22: The FortiGate-3140B in load balance mode

To enable this feature, issue this CLI command.

```
config system global
  set sp-load-balance enable
end
```

The FortiGate unit will then restart.

To return to the default mode, issue this CLI command.

```
config system global
  set sp-load-balance disable
end
```

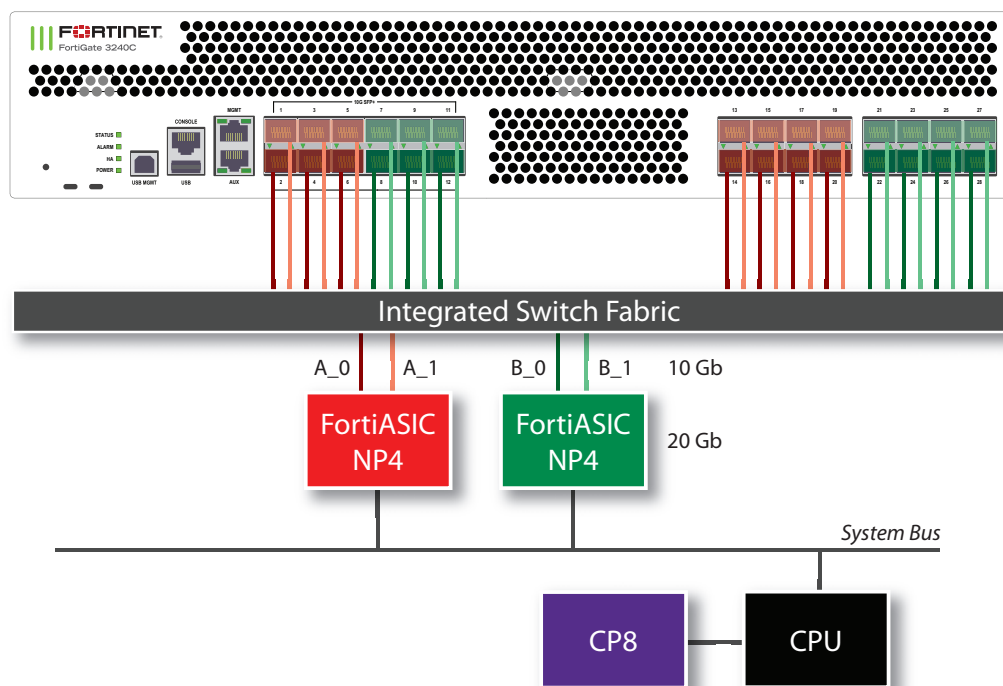
FortiGate-3240C

The FortiGate-3240C features two NP4 processors. Traffic between interfaces that use the same processor experience the highest acceleration.

- The 10 Gb interfaces, port1 through port6, and the 1 Gb interfaces, port13 through port20, share connections to one NP4 processor.
- The 10 Gb interfaces, port7 through port12, and the 1 Gb interfaces, port21 through port28, share connections to the other NP4 processor.

In addition to the ports being divided between the two NP4 processors, they are further divided between the two connections to each processor. Each NP4 can process 20 Gb of network traffic per second and each of two connections to each NP4 can move 10 Gb of data to the processor per second, so the ideal configuration would have no more than 10 Gb of network traffic to each connection of each NP4 at any time.

Figure 23 shows how the ports are connected to the NP4 processors.

Figure 23: The FortiGate-3240C

For example, for maximum NP4 acceleration of traffic received on port1, the traffic must exit the FortiGate-3240C unit on port2, port3, port4, port5, or port6 if the bandwidth exceeds 1 Gb. If the traffic bandwidth does not exceed 1 Gb, the traffic can also exit on port13 through port20. For maximum NP4 acceleration of traffic received on port7, the traffic must exit the FortiGate-3240C unit on port8, port9, port10, port11, or port12 if the bandwidth exceeds 1 Gb. If the traffic bandwidth does not exceed 1 Gb, the traffic can also exit on port21 through port28.

To maintain maximum throughput when adding more connections, ensure no more than 10 Gb of traffic is sent in and out (10 Gb in *and* 10 Gb out) of each of the two connections of each NP4 processor. Also ensure traffic enters and leaves the same processor.

FortiGate-3950B and FortiGate-3951B

The FortiGate-3950B features one NP4 processor to accelerate network traffic to wire speeds.

- The 1 Gb SPF interfaces, port1, port2, port3, port4, and the 10 Gb SPF+ interfaces, port5, port6, share connections to one NP4 processor.



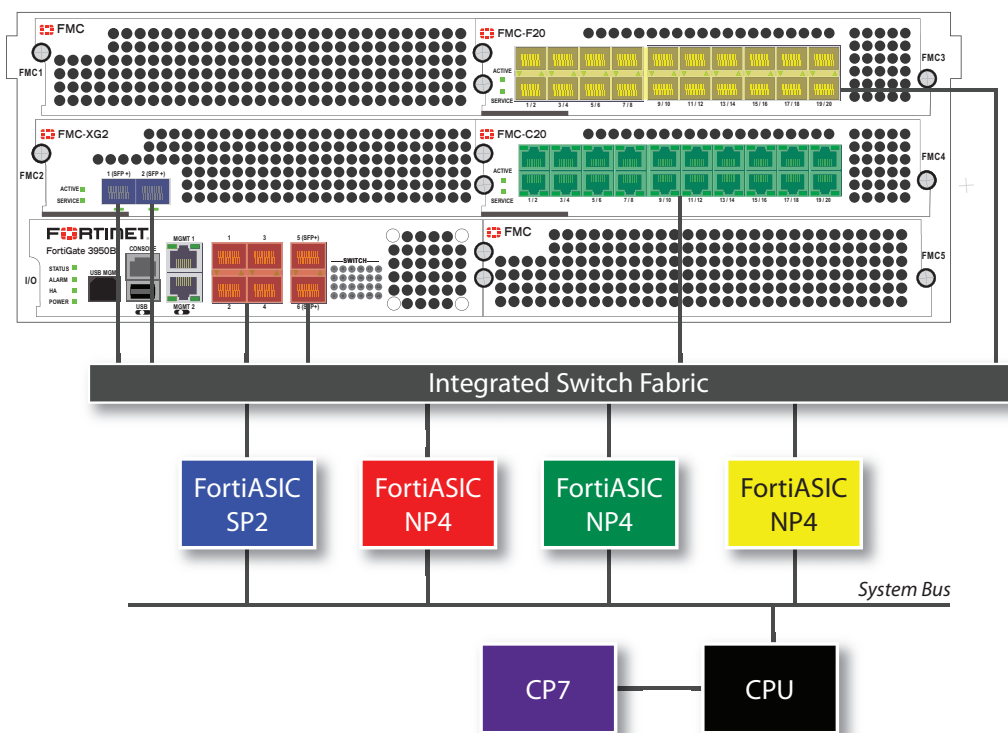
The FortiGate-3951B is similar to the FortiGate-3950B, except it trades one FMC slot for four FSM slots. The network interfaces available on each model are identical.

You can add additional FMC interface modules. If they support network traffic acceleration, it is only between interfaces on the module. [Figure 24](#) shows a FortiGate-3950B with three modules installed: an FMC-XG2, an FMC-F20, and an FMC-C20.

- The FMC-XG2 has one NP4 processor and one SP2 processor. The 10 Gb SPF+ interfaces, port1 and port2, share connections to both processors.

- The FMC-F20 has one NP4 processor and the twenty 1 Gb SPF interfaces, port1 through port20, share connections to the NP4 processor.
- The FMC-C20 has one NP4 processor and the twenty 10/100/1000 interfaces, port1 through port20, share connections to the NP4 processor.

Figure 24: The FortiGate-3950B with an FMC-XG2, an FMC-F20, and an FMC-C20



The processor in the FortiGate-3950B and on each FMC module can accelerate only the network traffic entering and leaving its own interfaces. For example, for maximum NP4 acceleration of traffic that exceeds 1 Gb bandwidth must enter and leave the FortiGate-3950B on its own port5 and port6, or the FMC-XG2 port1 and port2. If the traffic bandwidth does not exceed 1 Gb, the traffic can enter and exit using port1 through port4, or port1 through port20 on either the FMC-F20 or the FMC-C20.

Also, for maximum SP2 acceleration of traffic received on port1 of the FMC-XG2, the traffic must exit port2 of the FMC-XG2.

Traffic can enter an interface on one module and leaving an interface on another module, but it will not take advantage of any network or security acceleration.

FortiGate-3950B and FortiGate-3951B — load balance mode

Adding one or more FMC-XG2 modules to your FortiGate-3950B allows you to enable load balance mode. This feature allows you increased flexibility in how you use the interfaces on the FortiGate unit.

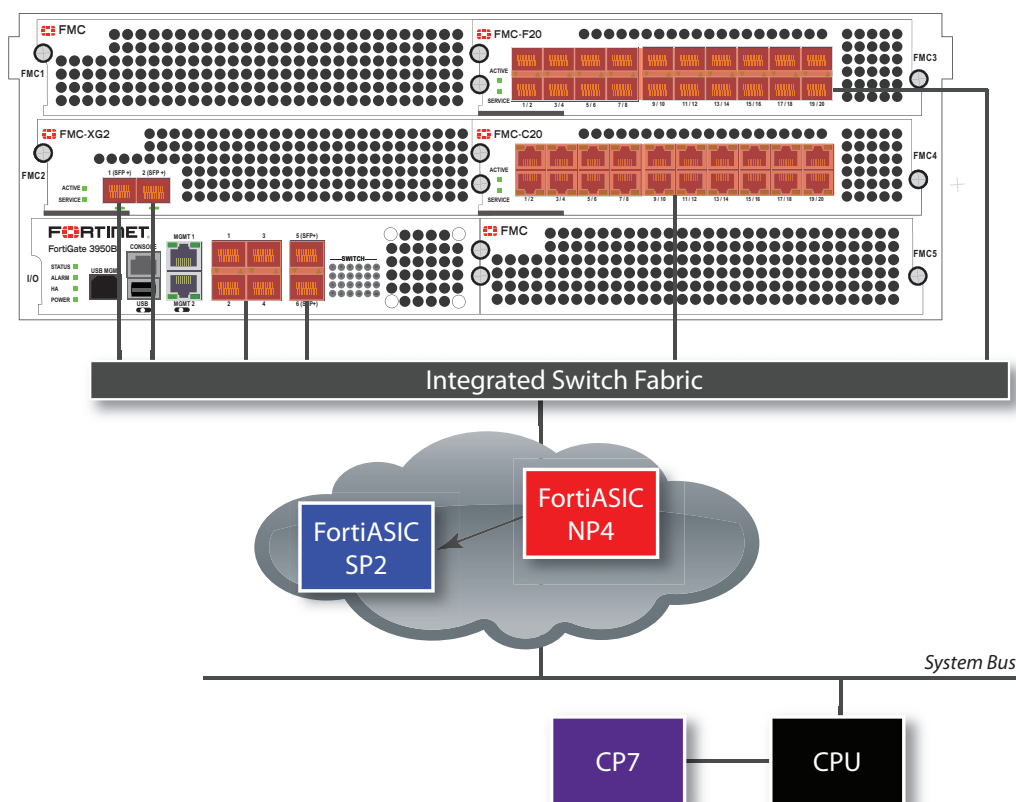


The FortiGate-3951B is similar to the FortiGate-3950B, except it trades one FMC slot for four FSM slots. The network interfaces available on each model are identical.

When enabled, traffic between any two interfaces (excluding management and console) is accelerated whether they are the six interfaces on the FortiGate-3950B itself, or on any installed FMC modules. Traffic is not limited to entering and leaving the FortiGate unit in specific interface groupings to benefit from NP4 and SP2 acceleration. You can use any pair of interfaces.

Security acceleration in this mode is limited, however. Only IPS scanning is accelerated in load balance mode.

Figure 25: The FortiGate-3950B in load balance mode



To enable this feature, issue this CLI command.

```
config system global
    set sp-load-balance enable
end
```

The FortiGate unit will then restart.

To return to the default mode, issue this CLI command.

```
config system global
    set sp-load-balance disable
end
```

Session offloading in HA active-active configuration

Fortinet's specialized network processors can improve network performance in active-active (load balancing) high availability (HA) configurations, even though traffic deviates from general offloading patterns, involving more than one network processor, each in a separate FortiGate unit. No additional offloading requirements apply.

Once the primary FortiGate unit's main processing resources send a session key to its network processor(s), network processor(s) on the primary unit can redirect any subsequent session traffic to other cluster members, reducing traffic redirection load on the primary unit's main processing resources.

As subordinate units receive redirected traffic, each network processor in the cluster assesses and processes session offloading independently from the primary unit. Session key states of each network processor are not part of synchronization traffic between HA members.

Configuring traffic shaping offloading

Accelerated Traffic shaping is supported with some limitations on NP2 and NP4 interfaces. Security processor modules do not perform any traffic shaping. Any traffic on which traffic shaping is enabled is handled by the FortiGate unit's main processing resources.

For traffic shaping and QoS through accelerated NP2 and NP4 ports,

- Accelerated ports support policy-based traffic policing. However, fast path traffic and traffic handled by the FortiGate CPU (slow path) are controlled separately, which means the policy setting on fast path does not consider the traffic on the slow path.
- The port based traffic policing as defined by the inbandwidth and outbandwidth CLI commands is not supported on the NP2 processor or the NP4 processor.
- NP2 and NP4 ports support DSCP configurations.
- Per-IP traffic shaping is not supported with NP2 interfaces due to hardware limitations.
- QoS in general is not supported by NP2 and NP4.

You can also use the traffic shaping features of the FortiGate unit's main processing resources by disabling the acceleration features of the NP2 and NP4 ports. See [“Disabling offloading” on page 39](#).

Network processing unit (`npu`) settings configure offloading for traffic shaping. Configured behavior applies to all network processors contained by the FortiGate unit itself or any installed AMC modules.

```
config system npu
    set traffic-shaping-mode {bidirection | unidirection}
```

end

Variables	Description	Default
traffic-shaping-mode {bidirection unidirection}	Select the offloaded traffic shaping bandwidth calculation method. unidirection: The bandwidth limit applies per direction. For example, a unidirectional limit of 10 KBps would result in an overall limit of 20 KBps — 10 KBps per direction. bidirection: The bandwidth limit applies to both directions overall. For example, a bidirectional limit of 10 KBps would result in an overall limit of 10 KBps — 5 KBps per direction. This option applies only if the FortiGate unit itself or any installed AMC modules contain a network processor that supports offloading of traffic shaping.	Varies by model.

Example

You could configure the traffic shaping limit to be applied as a bidirectional total limit during hardware accelerated sessions.

```
config system npu
  set traffic-shaping-mode bidirection
end

config system interface
  edit <interface_name>
    set outbandwidth <real outbandwidth>
  end
```

Checking that traffic is offloaded

You can determine whether traffic is offloaded by using the CLI command:

```
diagnose sys session list
```

The output provides detailed information about each session. Look for the “state=” line. If “npu npr” appears on that line, the session was offloaded to a network processor.

You can also use the diagnose command:

```
diagnose sniffer packet <interface_name>
```

Disabling offloading

If you want to completely disable offloading for test purposes or other reasons, you can do so by security policy.

```
config firewall policy
  edit <policy_id_int>
    set auto-asic-offload disable
  end
```

Multicast offloading / acceleration

Only security processor modules such as the CE4, CE8, or XE2 can offload multicast traffic from the FortiGate unit's CPU-based resources. To make use of this capability, the multicast traffic must enter and exit the FortiGate unit on network interfaces on the same SPM card. Also, the session fast path requirements must be met. These are the same requirements that apply to unicast traffic. See "[Session fast path requirements](#)" on [page 30](#).

Like any other traffic between interfaces, multicast traffic requires a firewall policy, in this case a multicast firewall policy. These policies, for example, permit multicast traffic between the first port and each of the other ports on an ASM-CE4 card:

```
config firewall multicast-policy
  edit 1
    set srcintf amc-sw1/1
    set dstintf amc-sw11/2
    set action accept
  next
  edit 2
    set srcintf amc-sw1/1
    set dstintf amc-sw11/3
    set action accept
  next
  edit 3
    set srcintf amc-sw1/1
    set dstintf amc-sw11/4
    set action accept
end
```

Note that simple forwarding of multicast packets is not accelerated. Also, if the FortiGate unit or VDOM is in Transparent mode, multicast is not accelerated.

Use `diagnose ip multicast npu-session list` to verify the NPU session is established

Configuring IPsec VPN offloading

Fortinet's specialized network processors contain features to improve IPsec tunnel performance. For example, network processors can encrypt and decrypt packets, reducing cryptographic load on the FortiGate unit's main processing resources.

IPsec offloading requirements

Requirements for hardware accelerated IPsec encryption or decryption are a modification of general offloading requirements. Differing characteristics are:

- origin can be local host (the FortiGate unit)
- in Phase I configuration, Local Gateway IP must be specified as an IP address of a network interface for a port attached to a network processor
- SA must have been received by the network processor

- in Phase II configuration:
 - encryption algorithm must be DES, 3DES, AES-128, AES-192, AES-256, or null
 - authentication must be MD5, SHA1, or null
 - if encryption is null, authentication must not also be null
 - if replay detection is enabled, `enc-offload-antireplay` must also be `enable` in the CLI



If replay detection is enabled in the Phase II configuration, you can enable or disable IPsec encryption and decryption offloading from the CLI. Performance varies by those CLI options and the percentage of packets requiring encryption or decryption. For details, see [“Configuring VPN encryption/decryption offloading” on page 41](#).



For session offloading to NP1 network processors, in Phase II configuration, the encryption algorithm must be 3DES and authentication must be MD5. Other encryption and authentication algorithms are not supported.

To apply hardware accelerated encryption and decryption, the FortiGate unit's main processing resources must first perform Phase I negotiations to establish the security association (SA). The SA includes cryptographic processing instructions required by the network processor, such as which encryption algorithms must be applied to the tunnel. After ISAKMP negotiations, the FortiGate unit's main processing resources send the SA to the network processor, enabling the network processor to apply the negotiated hardware accelerated encryption or decryption to tunnel traffic.

Possible accelerated cryptographic paths are:

- IPsec decryption offload
 - Ingress ESP packet > Offloaded decryption > Decrypted packet egress (fast path)
 - Ingress ESP packet > Offloaded decryption > Decrypted packet to FortiGate unit's main processing resources
- IPsec encryption offload
 - Ingress packet > Offloaded encryption > Encrypted (ESP) packet egress (fast path)
 - Packet from FortiGate unit's main processing resources > Offloaded encryption > Encrypted (ESP) packet egress

Configuring HMAC check offloading

Hash-based Message Authentication Code (HMAC) checks can be offloaded to network processors. To enable HMAC check offloading, enter

```
configure system global
  set ipsec-hmac-offload (enable|disable)
end
```

Configuring VPN encryption/decryption offloading

Network processing unit (npu) settings configure offloading behavior for IPsec VPN. Configured behavior applies to all network processors contained by the FortiGate unit itself or any installed AMC modules.

```
config system npu
  set enc-offload-antireplay {enable | disable}
  set dec-offload-antireplay {enable | disable}
  set offload-ipsec-host {enable | disable}
```

end

Variables	Description	Default
enc-offload-antireplay {enable disable}	Enable or disable offloading of IPsec encryption. This option is used only when replay detection is enabled in Phase II configuration. If replay detection is disabled, encryption is always offloaded.	disable
dec-offload-antireplay {enable disable}	Enable or disable offloading of IPsec decryption. This option is used only when replay detection is enabled in Phase II configuration. If replay detection is disabled, decryption is always offloaded.	enable
offload-ipsec-host {enable disable}	Enable or disable offloading of IPsec encryption of traffic from local host (FortiGate unit). Note: For this option to take effect, the FortiGate unit must have previously sent the security association (SA) to the network processor. For details on SA offloading, see “Configuring IPsec VPN offloading” on page 40 .	disable

Example

You could configure the offloading of encryption and decryption for an IPsec SA that was sent to the network processor.

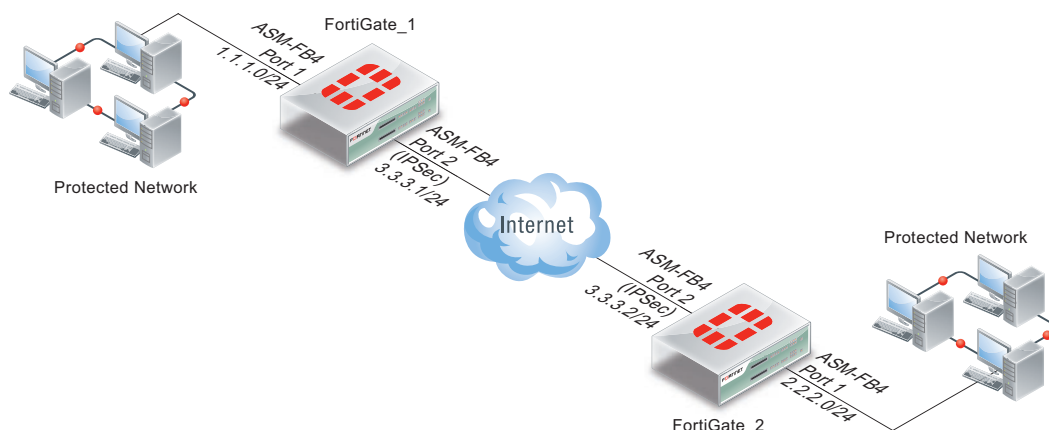
```
config system npu
  set enc-offload-antireplay enable
  set dec-offload-antireplay enable
  set offload-ipsec-host enable
end
```

Examples of ASM-FB4 accelerated VPNs

This section contains example IPsec configurations whose IPsec encryption and decryption processing is hardware accelerated by FortiGate-ASM-FB4 modules. [Figure 26](#) illustrates the example network topology. [Table 2](#) lists the example network interfaces and IP addresses.



Hardware accelerated IPsec does not require both tunnel endpoints to have the same network processor model. However, if hardware is not symmetrical, the packet forwarding rate is limited by the slower side.

Figure 26: Example network topology for offloaded IPsec processing**Table 2: Example ports and IP addresses for offloaded IPsec processing**

	FortiGate_1		FortiGate_2	
	Port	IP	Port	IP
IPsec tunnel	FortiGate-ASM-FB4 port 2	3.3.3.1/24	FortiGate-ASM-FB4 port 2	3.3.3.2/24
Protected network	FortiGate-ASM-FB4 port 1	1.1.1.0/24	FortiGate-ASM-FB4 port 1	2.2.2.0/24

Tunnel mode IPsec VPN example

The following steps create a hardware accelerated tunnel mode IPsec tunnel between two FortiGate units, each containing a FortiGate-ASM-FB4 module.

To configure hardware accelerated tunnel mode IPsec

- 1 On FortiGate_1, go to *VPN > IPsec*.
- 2 Configure Phase I.
For tunnel mode IPsec and for hardware acceleration, specifying the Local Gateway IP is required.
Select Advanced. In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.2, which is the IP address of FortiGate_2's FortiGate-ASM-FB4 module port 2.
- 3 Configure Phase II.
If you enable the check box "Enable replay detection," set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see ["Configuring VPN encryption/decryption offloading" on page 41](#).
- 4 Go to *Firewall > Policy*.
- 5 Configure one policy to apply the Phase 1 IPsec tunnel you configured in step 2 to traffic between FortiGate-ASM-FB4 module ports 1 and 2.
- 6 Go to *Router > Static*.

- 7 Configure a static route to route traffic destined for FortiGate_2's protected network to VPN IP address of FortiGate_2's VPN gateway, 3.3.3.2, through the FortiGate-ASM-FB4 module's port 2 (device).

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "AMC-SW1/2"
    set dst 2.2.2.0 255.255.255.0
    set gateway 3.3.3.2
  end
```

- 8 On FortiGate_2, go to *VPN > IPsec*.

- 9 Configure Phase I.

For tunnel mode IPsec and for hardware acceleration, specifying the Local Gateway IP is required.

Select Advanced. In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.1, which is the IP address of FortiGate_1's FortiGate-ASM-FB4 module port 2.

- 10 Configure Phase II.

If you enable the check box "Enable replay detection," set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see ["Configuring VPN encryption/decryption offloading" on page 41](#)

- 11 Go to *Firewall > Policy*.

- 12 Configure one policy to apply the Phase 1 IPsec tunnel you configured in step 9 to traffic between FortiGate-ASM-FB4 module ports 1 and 2.

- 13 Go to *Router > Static*.

- 14 Configure a static route to route traffic destined for FortiGate_1's protected network to VPN IP address of FortiGate_1's VPN gateway, 3.3.3.1, through the FortiGate-ASM-FB4 module's port 2 (device).

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "AMC-SW1/2"
    set dst 1.1.1.0 255.255.255.0
    set gateway 3.3.3.1
  end
```

- 15 Activate the IPsec tunnel by sending traffic between the two protected networks.

To verify tunnel activation, go to *VPN > IPSEC > Monitor*.

Interface mode IPsec VPN example

The following steps create a hardware accelerated interface mode IPsec tunnel between two FortiGate units, each containing a FortiGate-ASM-FB4 module.

To configure hardware accelerated interface mode IPsec

1 On FortiGate_1, go to *VPN > IPsec*.

2 Configure Phase I.

For interface mode IPsec and for hardware acceleration, the following settings are required.

- Select Advanced.
- Enable the check box “Enable IPsec Interface Mode.”
- In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.2, which is the IP address of FortiGate_2’s FortiGate-ASM-FB4 module port 2.

3 Configure Phase II.

If you enable the check box “Enable replay detection,” set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see [“Configuring VPN encryption/decryption offloading” on page 41](#)

4 Go to *Firewall > Policy*.

5 Configure two policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 2 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.

6 Go to *Router > Static*.

7 Configure a static route to route traffic destined for FortiGate_2’s protected network to the Phase 1 IPsec device, `FGT_1_IPsec`.

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "FGT_1_IPsec"
    set dst 2.2.2.0 255.255.255.0
  end
```

8 On FortiGate_2, go to *VPN > IPsec*.

9 Configure Phase I.

For interface mode IPsec and for hardware acceleration, the following settings are required.

- Enable the check box “Enable IPsec Interface Mode.”
- In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.1, which is the IP address of FortiGate_1’s FortiGate-ASM-FB4 module port 2.

10 Configure Phase II.

If you enable the check box “Enable replay detection,” set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see [“Configuring VPN encryption/decryption offloading” on page 41](#)

11 Go to *Firewall > Policy*.

12 Configure two policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 9 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.

13 Go to *Router > Static*.

- 14** Configure a static route to route traffic destined for FortiGate_1's protected network to the Phase 1 IPsec device, FGT_2_IPsec.

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "FGT_2_IPsec"
    set dst 1.1.1.0 255.255.255.0
  next
end
```

- 15** Activate the IPsec tunnel by sending traffic between the two protected networks.

To verify tunnel activation, go to *VPN > IPSEC > Monitor*.

Configuring IPS offloading

Security modules may offload IPS functions. The requirements to achieve this are:

- Source interface is on a SP module.
- Destination interface is on the same SP module.
- UTM configuration must enable only IPS, not AV or DLP.
- Packet protocol is ICMP, UDP or TCP.

IPS offloading functions with policy-based IPS and sniffer-policy mode.

Interface-based policies are offloaded if only a DoS sensor is configured. If any other sensors are selected in the Interface-based policy, even if their actions are set to 'Pass,' all of the matching traffic will be handled by the FortiGate unit CPU, and not offloaded to the SP module.

Configuring pre-IPS anomaly detection

Network interfaces associated with a port attached to a network processor can be configured to use hardware acceleration to drop or allow certain anomaly types, separately from and in advance of any anomaly checks specified by Intrusion Prevention (IPS). Configured behavior applies separately to each of these network interfaces.

```
config system interface
  edit <name_str>
    set fp-anomaly
      {drop_icmpland | pass_icmpland}
      {drop_ipland | pass_ipland}
      {drop_iplsrr | pass_iplsrr}
      {drop_iprr | pass_iprr}
      {drop_ipsecurity | pass_ipsecurity}
      {drop_ipssrr | pass_ipssrr}
      {drop_ipstream | pass_ipstream}
      {drop_iptimestamp | pass_iptimestamp}
      {drop_ipunknown_option | pass_ipunknown_option}
      {drop_unknown_prot | pass_ipunknown_prot}
      {drop_tcpland | pass_tcpland}
      {drop_udpland | pass_udpland}
      {drop_winnuke | pass_winnuke}
  end
```

where:

icmpland	ICMP land
ipland	IP land
iplsrr	IP with loose source record route
iprr	IP with record route option
ipsecurity	IP with security option
ipssrr	IP with strict source record route option
ipstream	IP with stream option
iptimestamp	IP with timestamp option
ipunknown_option	IP with unknown option
ipunknown_prot	IP with unknown protocol
tcpland	TCP land
udpland	UDP land
winnuke	TCP WinNuke

Example

You might configure a FortiGate-ASM-FB4 module to drop packets with TCP WinNuke or unknown IP protocol anomalies, but to pass packets with an IP time stamp, using hardware acceleration provided by the network processor.

```
config system interface
  edit AMC-SW1/1
    set fp-anomaly drop_winnuke drop_ipunknown_prot
    pass_iptimestamp
  end
```

Configuring policy-based IPS on SP modules

In the firewall policy, enable UTM, then enable IPS and select the desired IPS profile.

Configuring interface-based IPS on SP modules

- 1 Define the IPS sensor. This step is the same with current policy-based IPS. For system predefined sensor, this step can be ignored.
- 2 Define on which interface IPS should be enabled and what sensor you want to use to scan traffic. Both physical interface and VLAN interface are valid interface choices.

The followed is an example to enable IPS sensor “all_default” on physical port AMC-SW1/2.

```
config ips interface
  edit AMC-SW1/2
    set ips-sensor all_default
  end
```

This command will enable IPS on all traffic ingress and egress through AMC-SW1/2.

Do not enable policy-based IPS when either the source or destination port has interface IPS enabled. Doing so provides no additional security and results in reduced performance.

Examples

Hardware accelerated IPsec processing, involving either partial or full offloading, can be achieved in either tunnel or interface mode IPsec configurations.

To achieve offloading for both encryption and decryption:

- In Phase I configuration’s Advanced section, Local Gateway IP must be specified as an IP address of a network interface associated with a port attached to a network processor. (In other words, if Phase 1’s Local Gateway IP is Main Interface IP, or is specified as an IP address that is not associated with a network interface associated with a port attached to a network processor, IPsec network processing is not offloaded.)
- In Phase II configuration’s P2 Proposal section, if the checkbox “Enable replay detection” is enabled, `enc-offload-antireplay` and `dec-offload-antireplay` must be set to enable in the CLI.
- `offload-ipsec-host` must be set to enable in the CLI.

This section contains example IPsec configurations whose IPsec encryption and decryption processing is hardware accelerated by FortiGate-ASM-FB4 modules. [Figure 26](#) illustrates the example network topology. [Table 2](#) lists the example network interfaces and IP addresses.



Hardware accelerated IPsec does not require both tunnel endpoints to have the same network processor model. However, if hardware is not symmetrical, the packet forwarding rate is limited by the slower side.

Figure 27: Example network topology for offloaded IPsec processing

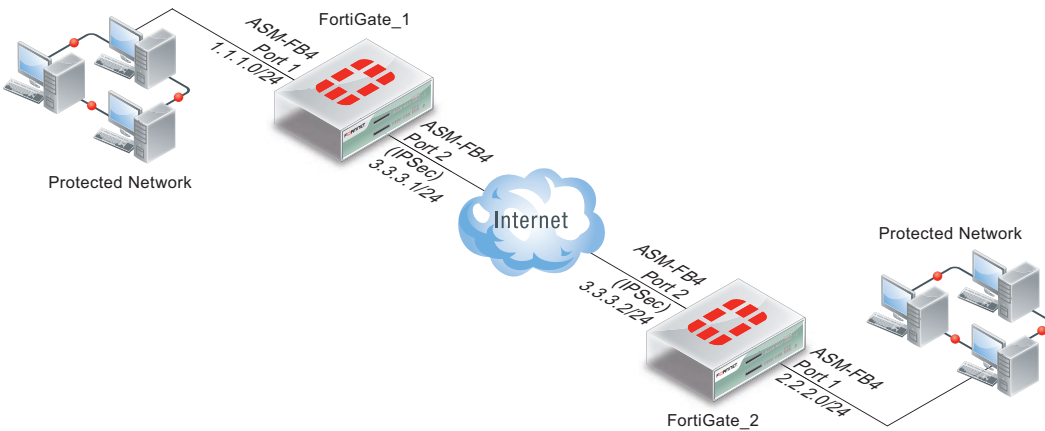


Table 3: Example ports and IP addresses for offloaded IPsec processing

	FortiGate_1		FortiGate_2	
	Port	IP	Port	IP
IPsec tunnel	FortiGate-ASM-FB4 port 2	3.3.3.1/24	FortiGate-ASM-FB4 port 2	3.3.3.2/24

Table 3: Example ports and IP addresses for offloaded IPsec processing

Protected network	FortiGate-ASM-FB4 port 1	1.1.1.0/24	FortiGate-ASM-FB4 port 1	2.2.2.0/24
--------------------------	--------------------------	------------	--------------------------	------------

This section includes the following topics:

- [Tunnel mode IPsec VPN example](#)
- [Configuring traffic offloading](#)

Accelerated tunnel mode IPsec

The following steps create a hardware accelerated tunnel mode IPsec tunnel between two FortiGate units, each containing a FortiGate-ASM-FB4 module.

To configure hardware accelerated tunnel mode IPsec

- 1 On FortiGate_1, go to *VPN > IPsec*.
- 2 Configure Phase I.
For tunnel mode IPsec and for hardware acceleration, specifying the Local Gateway IP is required.
Select Advanced. In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.2, which is the IP address of FortiGate_2's FortiGate-ASM-FB4 module port 2.
- 3 Configure Phase II.
If you enable the checkbox "Enable replay detection," set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see "[Configuring VPN encryption/decryption offloading](#)" on page 41
- 4 Go to *Firewall > Policy*.
- 5 Configure one policy to apply the Phase 1 IPsec tunnel you configured in step 2 to traffic between FortiGate-ASM-FB4 module ports 1 and 2.
- 6 Go to *Router > Static*.
- 7 Configure a static route to route traffic destined for FortiGate_2's protected network to VPN IP address of FortiGate_2's VPN gateway, 3.3.3.2, through the FortiGate-ASM-FB4 module's port 2 (device).

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "AMC-SW1/2"
    set dst 2.2.2.0 255.255.255.0
    set gateway 3.3.3.2
  end
```

- 8 On FortiGate_2, go to *VPN > IPsec*.
- 9 Configure Phase I.
For tunnel mode IPsec and for hardware acceleration, specifying the Local Gateway IP is required.
Select Advanced. In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.1, which is the IP address of FortiGate_1's FortiGate-ASM-FB4 module port 2.

10 Configure Phase II.

If you enable the checkbox “Enable replay detection,” set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see [“Configuring VPN encryption/decryption offloading” on page 41](#)

11 Go to *Firewall > Policy*.**12** Configure one policy to apply the Phase 1 IPsec tunnel you configured in step 9 to traffic between FortiGate-ASM-FB4 module ports 1 and 2.**13** Go to *Router > Static*.**14** Configure a static route to route traffic destined for FortiGate_1’s protected network to VPN IP address of FortiGate_1’s VPN gateway, 3.3.3.1, through the FortiGate-ASM-FB4 module’s port 2 (device).

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "AMC-SW1/2"
    set dst 1.1.1.0 255.255.255.0
    set gateway 3.3.3.1
  end
```

15 Activate the IPsec tunnel by sending traffic between the two protected networks.

To verify tunnel activation, go to *VPN > IPSEC > Monitor*.

Accelerated interface mode IPsec

The following steps create a hardware accelerated interface mode IPsec tunnel between two FortiGate units, each containing a FortiGate-ASM-FB4 module.

To configure hardware accelerated interface mode IPsec

1 On FortiGate_1, go to *VPN > IPsec*.**2** Configure Phase I.

For interface mode IPsec and for hardware acceleration, the following settings are required.

- Select Advanced.
- Enable the checkbox “Enable IPsec Interface Mode.”
- In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.2, which is the IP address of FortiGate_2’s FortiGate-ASM-FB4 module port 2.

3 Configure Phase II.

If you enable the checkbox “Enable replay detection,” set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see [“Configuring VPN encryption/decryption offloading” on page 41](#)

4 Go to *Firewall > Policy*.**5** Configure two policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 2 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.**6** Go to *Router > Static*.

- 7** Configure a static route to route traffic destined for FortiGate_2's protected network to the Phase 1 IPsec device, FGT_1_IPsec.

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "FGT_1_IPsec"
    set dst 2.2.2.0 255.255.255.0
  end
```

- 8** On FortiGate_2, go to *VPN > IPsec*.

- 9** Configure Phase I.

For interface mode IPsec and for hardware acceleration, the following settings are required.

- Enable the checkbox "Enable IPsec Interface Mode."
- In the Local Gateway IP section, select Specify and type the VPN IP address 3.3.3.1, which is the IP address of FortiGate_1's FortiGate-ASM-FB4 module port 2.

- 10** Configure Phase II.

If you enable the checkbox "Enable replay detection," set `enc-offload-antireplay` to `enable` in the CLI. For details on encryption and decryption offloading options available in the CLI, see ["Configuring VPN encryption/decryption offloading" on page 41](#)

- 11** Go to *Firewall > Policy*.

- 12** Configure two policies (one for each direction) to apply the Phase 1 IPsec configuration you configured in step 9 to traffic leaving from or arriving on FortiGate-ASM-FB4 module port 1.

- 13** Go to *Router > Static*.

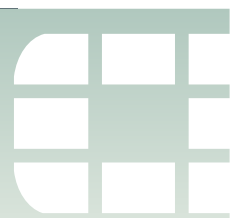
- 14** Configure a static route to route traffic destined for FortiGate_1's protected network to the Phase 1 IPsec device, FGT_2_IPsec.

You can also configure the static route using the following CLI commands:

```
config router static
  edit 2
    set device "FGT_2_IPsec"
    set dst 1.1.1.0 255.255.255.0
  next
end
```

- 15** Activate the IPsec tunnel by sending traffic between the two protected networks.

To verify tunnel activation, go to *VPN > IPSEC > Monitor*.



Configuring RAID

This section describes how to configure RAID on a FortiGate unit with multiple disk support. RAID arrays can provide faster disk access, redundancy in case of partial failure, or both depending on the RAID level you select.

The following topics are included in this section:

- [RAID levels](#)
- [Configuring a RAID array](#)
- [Checking the status of a RAID array](#)
- [Rebuilding a RAID array](#)

RAID levels

Some FortiGate models have two or more hard disks configured in a RAID array to store log messages locally on the FortiGate unit. A RAID array can provide faster disk access, redundancy in case of partial failure, or both depending on the RAID level you select.

When changing the RAID level, the available levels depend on the number of working disks that are actually present in the unit. For example, RAID-5 is not available on units with fewer than three disks. When a disk fails, becomes corrupt, or is removed you must rebuild the RAID array. For more information, see [“Rebuilding a RAID array” on page 56](#).

If the FortiGate unit has only one disk installed, the RAID monitor widget will not be displayed as it is not possible to configure a RAID array with only one disk.

Available RAID levels include:

- [RAID-0](#)
- [RAID-1](#)
- [RAID-5](#)

RAID-0

A RAID-0 array is also referred to as striping. The FortiGate unit writes information evenly across all hard disks. The total space available is that of all the disks in the RAID array. There is no redundancy available. If any single drive fails, the data on the array is lost and cannot be recovered. Because of this lack of redundancy, a RAID-0 array will never report a degraded condition. This RAID level is beneficial because it provides better performance, since the FortiGate unit can distribute disk writing across multiple disks.

For example if your FortiGate unit has three disks each with a 1 terabyte (TB) capacity, your RAID-0 array will have a 3TB capacity.

RAID-1

A RAID-1 array is also referred to as mirroring. The FortiGate unit writes information to one hard disk, and writes a copy (a mirror image) of all information to all other hard disks. The total disk space available is that of only one hard disk, as the others are solely used for mirroring. This provides redundant data storage. Should any of the hard disks fail, there one or more backup hard disks available. For example, if one disk fails, the unit can still access three other hard disks and continue functioning.

RAID-5

A RAID-5 array employs striping with a parity check. Similar to RAID-0, the FortiGate unit writes information evenly across all drives but additional parity blocks are written on the same stripes. The parity block is staggered for each stripe. RAID-5 requires three or more hard disks. The total disk space is the total number of disks in the array, minus the capacity of one disk for parity storage. For example, with four hard disks, the total capacity available is the capacity of three hard disks. RAID-5 performance is typically better with reading than with writing, although performance is degraded when one disk has failed. With RAID-5, one disk can fail without the loss of data. If a drive fails, it can be replaced and the FortiGate unit will restore the data on the new disk by using reference information from the parity volume.

Configuring a RAID array



Do not remove a disk while the RAID array is synchronizing — you may lose stored information. This will also degrade the array, requiring a rebuild.

A RAID array provides no redundancy in a degraded state. Any disk failure while the RAID is in a degraded state will cause data loss.

When switching RAID levels, you may see the message “RAID status is OK and RAID is doing background synchronization.” Synchronization of the disks in the array will take considerable time — it will take longer for larger arrays and for disks with more storage capacity.

To configure a RAID array

- 1 Go to *System > Dashboard > Status* where the RAID Monitor widget is located, and then select *Configure* in the widget title bar area.



Changing the RAID level will erase any stored log information on the array, and reboot the FortiGate unit. The unit will remain offline while it reconfigures the RAID array. When it reboots, the array will need to synchronize before being fully operational.

- 2 Confirm that the FortiGate unit recognizes the installed hard disks. Each slot in which you have installed a hard disk displays a green check mark for *Member* and OK for *Status*. The Capacity figure for each hard disk simply lists its size.

The available space on the array will depend on the size of the member drives, but it may not be equal to the total size of the member drives. Further, the hard disks in a RAID array need to have the same capacity. If you use disks with differing capacities, the member hard disks will be treated as if they all have the capacity of the smallest drive in the array. The RAID level determines how the size of the RAID array relates to the size of the member hard disks. For example, an array of three 1TB hard disks will result in 3TB of usable space with RAID-0, 2TB of usable space with RAID-5, and 1TB of space with RAID-1.

3 Select the RAID level.

RAID-0 (Striping)	Better performance than a single disk, but no redundancy. If either disk fails, all data is lost.
RAID-1 (mirroring)	Performance comparable to a single disk, and data is protected by redundancy. One disk can fail with no data loss.
RAID-5 (striping with parity)	Performance is mixed with disk writes slower than a single disk and disk reads faster. Data is protected by redundancy. One disk can fail with no data loss.

For more information on RAID levels, see [“RAID levels” on page 53](#).

4 Select *Apply*.

The FortiGate unit reboots and reconfigures the RAID array. You may log in again when it is complete.

Checking the status of a RAID array

Once a RAID array is configured, it requires no regular maintenance. Attention is required only when a member hard drive fails. The RAID widget reports the RAID array condition and disk space utilization.

To check the status of a RAID array

- 1 Go to *System > Dashboard > Status* where the RAID Monitor widget is located.
- 2 The widget shows three pieces of status information about the RAID array.

Array Status	Displays the RAID level and status of the RAID array. The hard disks installed in the FortiGate unit are also displayed, with indicators to show which are part of the RAID array and the status of each disk. The status can be: OK — standard status, everything is normal OK (Background-Synchronizing) (%) — synchronizing the disks after changing RAID level, Synchronizing progress bar shows percent complete Degraded — One or more of the disks in the array has failed, been removed, or is not working properly. A warning is displayed about the lack of redundancy in this state. Also, a degraded array is slower than a healthy array. Select <i>Rebuild RAID</i> to fix the array after replacing the defective or missing disk. Degraded (Background-Rebuilding) (%) — The same as degraded, but the RAID array is being rebuilt in the background. The array continues to be in a fragile state until the rebuilding is completed.
---------------------	---

Disk Space Usage	Shows a bar graph of the used space as well as text listing the used space, free space, and total disk space available in the array.
Synchronize Status	Shows that the array is synchronized or reports the synchronization progress, as well as any information about the current synchronization status.

Rebuilding a RAID array

A RAID array has multiple disks with writing to the disks being spread out so that if one disk in the array fails, the array can still provide all the stored information. Some forms of RAID do not provide redundancy, however most do.

When a disk fails, or the RAID array becomes degraded

The Alert Message Console widget, located in *System > Dashboard > Status*, displays any messages about events or activities that need urgent attention, such as a failed hard disk. This widget provides detailed messages that contain the date and time of the event or activity, as well as an explanation about what happened.

Why rebuild a RAID array?

When the RAID array has redundancy and one disk in the array fails, becomes corrupted, or is removed the array becomes degraded. In a degraded state the array can still function, but there are some changes. The two main changes are that there is no longer redundancy and accessing the array takes longer than before.

There is no redundancy because with one disk removed from the array, the information that was stored on that disk can be retrieved using the other disks in the array. However, removing another disk from the array would remove information that has no backup or parity data. This second disk's removal would result in data loss and the array will fail. This delicate state of the RAID array is displayed in the warning message on the dashboard RAID monitor when the status is degraded in the form of a warning.

The array takes longer to access data because instead of the data being retrieved in the format and order it is expected, the array has to jump around to find it and at times recreate the missing data from the parity information. This all takes longer than just the usual straight read operation and will continue until the RAID array has been rebuilt.

The reasons you rebuild a RAID array include:

- a disk has failed
- the array has become corrupted
- a disk has been removed

How to rebuild the RAID array

When the RAID array is in its normal OK state, there is no option to rebuild the array because there is no need for it. You only need to rebuild the array when it is in a degraded state and in danger of losing data.

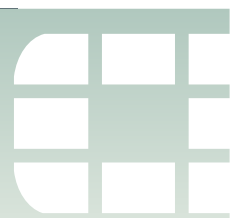
Before you rebuild the RAID array, you should have a replacement disk for the one that failed if that is the cause of the degraded array. You cannot rebuild an array that is missing a disk. A replacement disk should be the same storage capacity as the disk it is replacing.

Also before rebuilding the array, you should backup the data if possible. As soon as the RAID array becomes degraded you should backup the array if possible to prevent data loss.

To rebuild the RAID array

- 1 Go to *System > Dashboard > Status*, and then in the RAID Monitor widget, select *[Configure]*.
- 2 Verify the status of the RAID array is degraded, and the Rebuild button is not greyed out.
- 3 Remove the failed disk from the FortiGate unit.
 - Ensure you have the correct disk.
 - Press the green button to unlock the disk.
 - Gently push the lever to the left as far as it will go to disconnect the disk.
 - Remove the disk from the FortiGate unit by pulling on the lever.
- 4 Insert the new disk into the FortiGate unit that is replacing the failed disk.
 - Insert the disk carefully into the FortiGate unit.
 - Push the front panel of the disk to make the connection—the lever will start to move to the right. Ensure that both sides of the disk are in line with the other disks.
 - When in place push the bar fully to the right, until the green button clicks.
- 5 Refresh your display to ensure the new disk is installed properly. If it is not recognized, repeat steps 3 and 4 with the new disk to ensure it is properly installed.
- 6 On the configure screen, select *Rebuild RAID*.

Rebuilding the RAID array will normally take several hours. You can follow its progress on the RAID Monitor display on the dashboard.
- 7 When the rebuild is complete, the status of the RAID array will change to OK.



FortiBridge installation and operation

This chapter describes a typical transparent mode FortiGate network and how to add a FortiBridge unit to this network to provide fail open protection. This chapter also contains detailed information about how FortiBridge units operate and concludes with descriptions of adding a FortiBridge unit to an HA cluster and connecting a FortiBridge unit other FortiGate interfaces.

This chapter contains the following sections:

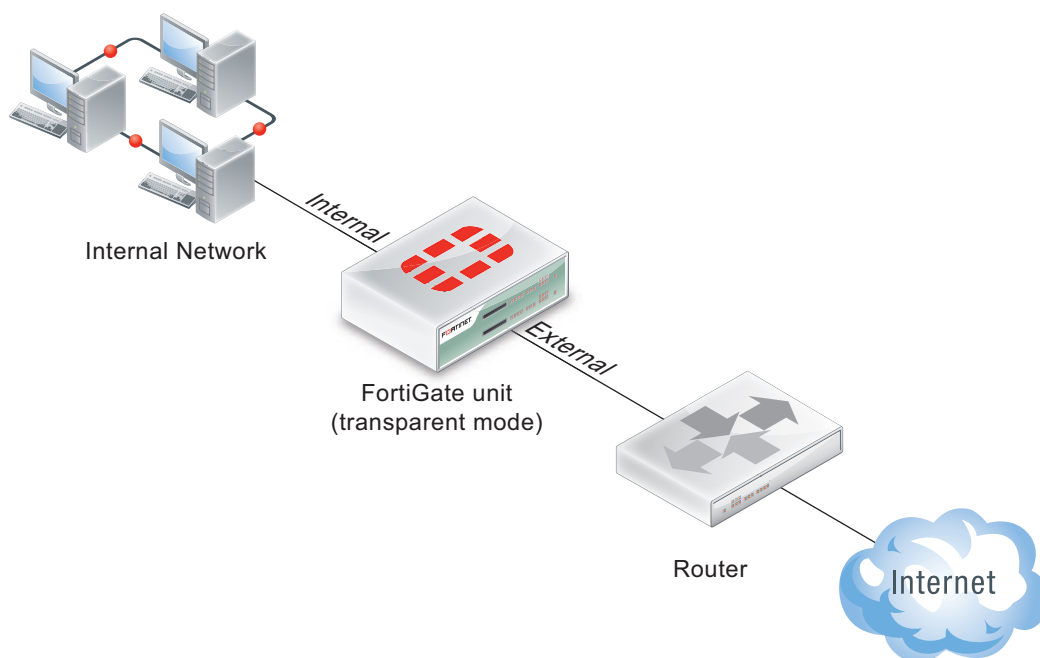
- [Example FortiBridge application](#)
- [Normal mode operation](#)
- [Bypass mode operation](#)
- [FortiBridge power failure](#)
- [Example FortiGate HA cluster FortiBridge application](#)
- [Example configuration with other FortiGate interfaces](#)

Example FortiBridge application

A typical application of a FortiGate unit operating in transparent mode is to insert the FortiGate unit into an internal network, between the network and the router that connects the network to the Internet. In this configuration, the FortiGate unit can provide security services for all traffic passing between the internal network and the internet. These security services can include:

- applying firewall policies and IPS attack prevention to all traffic,
- applying virus scanning to HTTP, FTP, POP3, SMTP, and IMAP traffic,
- applying web filtering to HTTP traffic,
- applying Spam filtering to POP3, SMTP, and IMAP traffic.

The internal network is connected to the FortiGate unit internal interface. The router is connected to the FortiGate unit external interface. The FortiGate unit can be added to the network without changing the configuration of the network (except to add the FortiGate management IP address).

Figure 28: Example transparent mode network

To allow users on the internal network to connect to resources on the Internet, add Internal → External firewall policies to the FortiGate unit. Add protection profiles to the firewall policies to apply security services such as virus scanning, web filtering, spam filtering and IPS to the traffic that passes through the FortiGate unit.

The FortiGate unit acts as an extra layer of protection for your internal network. While it is operating, the FortiGate unit protects the internal network from threats originating on the Internet. All users on the internal network connect through the FortiGate unit to the Internet. This also means that if a failure or other interruption caused the FortiGate unit to stop functioning, users on the internal network would not be able to connect to the Internet.

You can install a FortiBridge unit to maintain internet connectivity for the internal network if the FortiGate unit stops functioning. The FortiBridge unit provides fail open protection for your network by bypassing the FortiGate unit if a failure occurs.

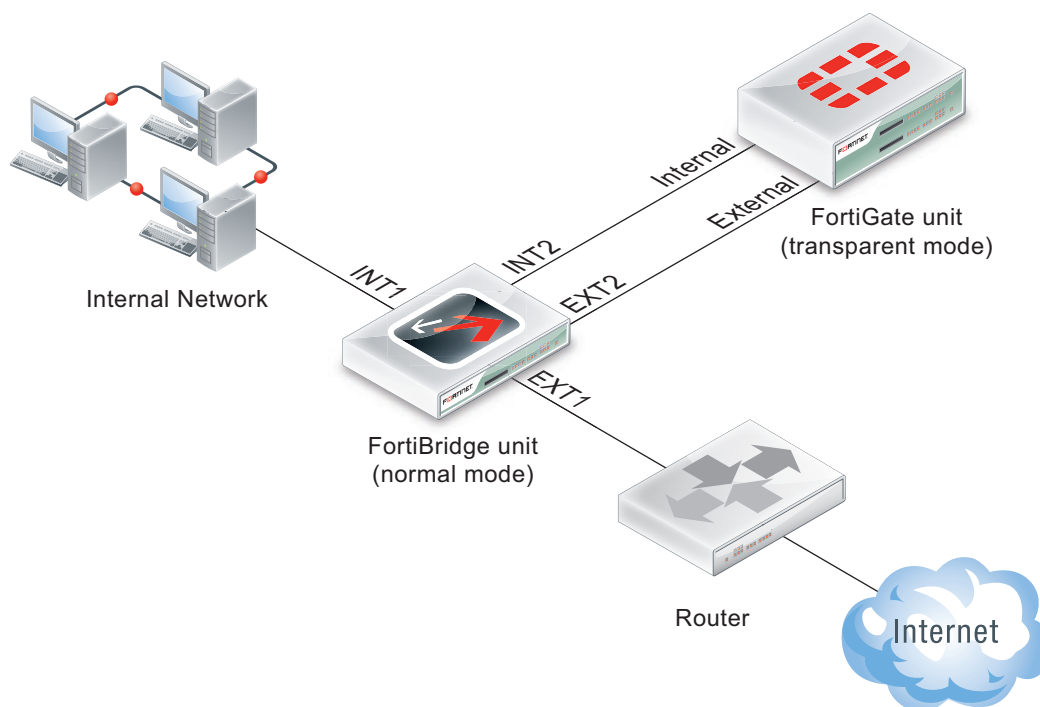
Connecting the FortiBridge unit

Operating in normal mode, the FortiBridge unit functions like a layer-2 bridge, passing all traffic to the FortiGate unit. The FortiGate unit processes the traffic, which passes through the FortiBridge unit again and then to its final destination.

In most cases, you do not have to make changes to the FortiGate unit configuration or to the network to add a FortiBridge unit. The only network requirement for FortiBridge is the availability of a single management IP address for the FortiBridge unit. The FortiBridge management IP address is required in addition to the FortiGate management IP address.

The connection procedure is different depending on whether the FortiBridge unit uses copper gigabit ethernet network connections or fiber gigabit ethernet network connections. This section includes the following connection procedures:

- [Connecting the FortiBridge-2002 \(copper gigabit ethernet\)](#)
- [Connecting the FortiBridge-2002F \(fiber gigabit ethernet\)](#)

Figure 29: FortiBridge unit providing fail open protection

Connecting the FortiBridge-2002 (copper gigabit ethernet)

The FortiBridge-2002 unit contains 4 auto-sensing 10/100/1000 Ethernet interfaces that connect to the internal and external networks and to the FortiGate interfaces that were connected to these networks. Use the following steps to connect a FortiBridge-2002 unit to the network as shown in [Figure 29](#).



Normally, you would use straight-through ethernet cables to connect the FortiBridge-2002 unit to the FortiGate unit and to your networks. However, for some connections you may need a crossover ethernet cable (for example, for compatibility with network devices that do not support Auto MDI/MDIX).

- 1 Connect the FortiBridge-2002 INT2 interface to the FortiGate internal interface.
- 2 Connect the FortiGate external interface to the FortiBridge-2002 EXT2 interface.
- 3 Connect the internal network to the FortiBridge-2002 INT1 interface.
- 4 Connect the FortiBridge-2002 EXT1 interface to the router.

Connecting the FortiBridge-2002F (fiber gigabit ethernet)

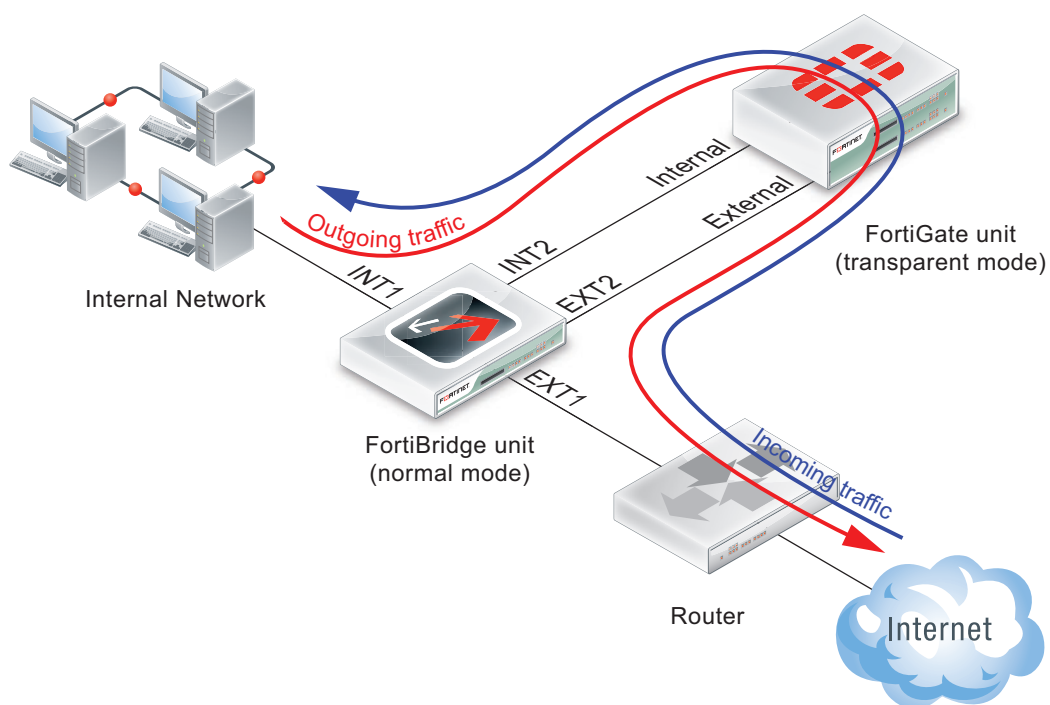
The FortiBridge-2002F unit contains 4 multimode fiber optic gigabit interfaces that connect to the internal and external networks and to the FortiGate interfaces that were connected to these networks. Use the following steps to connect a FortiBridge-2002F unit to the network as shown in [Figure 29](#).

- 1 Connect the FortiBridge-2002F INT2 interface to the FortiGate internal interface.
- 2 Connect the FortiGate external interface to the FortiBridge-2002F EXT2 interface.
- 3 Connect the internal network to the FortiBridge-2002F INT1 interface.
- 4 Connect the FortiBridge-2002F EXT1 interface to the router.

Normal mode operation

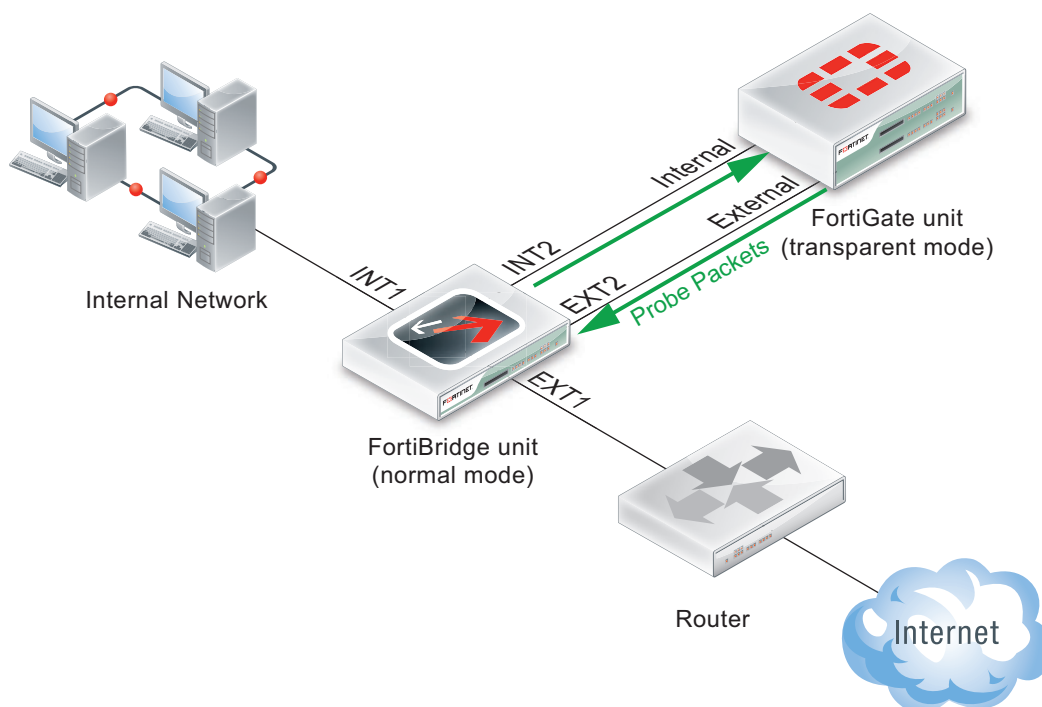
If the FortiGate unit is processing traffic normally, the FortiBridge unit operates in Normal mode. Traffic from the internal network enters the FortiBridge INT1 interface then exits the INT2 interface to the FortiGate unit. The traffic from the FortiBridge INT2 interface enters the FortiGate internal interface. Firewall policies and protection profiles are applied to the traffic by the FortiGate unit. Accepted traffic exits the FortiGate External interface and enters the FortiBridge EXT2 interface. The traffic then exits the FortiBridge EXT1 interface and goes to the external network. Traffic from the external network follows this sequence in the opposite direction.

Figure 30: Normal mode traffic flow



How the FortiBridge unit monitors the FortiGate unit

To monitor the FortiGate unit for failure, you must enable probes on the FortiBridge unit. When you enable a probe, the FortiBridge unit sends packets from the FortiBridge INT2 interface, through the FortiGate unit to the FortiBridge EXT2 interface. If the EXT2 interface receives the probe packets, the FortiGate unit is operating normally. If the EXT2 interface does not receive probe packets the FortiBridge unit assumes that the FortiGate unit has failed.

Figure 31: FortiBridge unit operating in normal mode sending probe packets

You can enable ICMP (ping), HTTP, FTP, POP3, SMTP, and IMAP probes to test connectivity through the FortiGate unit for each of these protocols. The FortiBridge unit simultaneously tests connectivity through the FortiGate unit for each probe that is enabled.

The first probe that registers a failure causes the FortiBridge unit to stop sending all probe packets. The FortiBridge unit responds to the failure according to the action on failure that you configure. The action on failure can include fail open, send alert email, send a syslog message, and send an SNMP trap. You can enable any combination of these actions on failure. Fail open switches the FortiBridge unit to bypass mode. Other actions on failure alert system administrators that the FortiBridge has determined that a failure occurred.

Probes and FortiGate firewall policies

Probe packets are accepted and passed through the FortiGate unit by firewall policies added to the FortiGate unit. When enabling probes, you must make sure that the firewall policies added to the FortiGate unit can accept probe packets. For example, if your FortiGate unit does not accept FTP packets, you should not enable the FTP probe. [Table 4](#) describes FortiGate firewall policy requirements for each FortiBridge probe.

Table 4: FortiBridge probes and FortiGate firewall policy requirements

Probe	Description	FortiGate Firewall policy	
		Direction	Service
Ping	ICMP packets are sent from the INT2 interface to the EXT2 interface. The EXT2 interface responds to the ping.	Internal -> External	ICMP or ANY

Table 4: FortiBridge probes and FortiGate firewall policy requirements (Continued)

Probe	Description	FortiGate Firewall policy	
		Direction	Service
HTTP	HTTP requests are sent from an HTTP client at the INT2 interface to a web server at the EXT2 interface. The web server sends a response from the EXT2 interface to the INT2 interface.	Internal -> External	HTTP or ANY
SMTP	SMTP packets are sent from an SMTP server at the INT2 interface to an SMTP server at the EXT2 interface. The SMTP server sends a response from the EXT2 interface to the INT2 interface.	Internal -> External	SMTP or ANY
POP3	POP3 packets are sent from a POP3 client at the INT2 interface to a POP3 server at the EXT2 interface. The POP3 server sends a response from the EXT2 interface to the INT2 interface.	Internal -> External	POP3 or ANY
IMAP	IMAP packets are sent from an IMAP client at the INT2 interface to an IMAP server at the EXT2 interface. The IMAP server sends a response from the EXT2 interface to the INT2 interface.	Internal -> External	IMAP or ANY
FTP	FTP requests are sent from an FTP client at the INT2 interface to an FTP server at the EXT2 interface. The FTP server sends a response from the EXT2 interface to the INT2 interface.	Internal -> External	FTP or ANY
mm1	MM1 packets are sent from the INT2 interface to the EXT2 interface, through the FortiGate unit. When the packet is received, an MM1 response is sent back from the EXT2 interface to the INT2 interface.	Internal -> External	custom or ANY
mm3	MM3 packets are sent from the INT2 interface to the EXT2 interface, through the FortiGate unit. When the packet is received, an MM3 response is sent back from the EXT2 interface to the INT2 interface.	Internal -> External	custom or ANY
mm4	MM4 packets are sent from the INT2 interface to the EXT2 interface, through the FortiGate unit. When the packet is received, an MM4 response is sent back from the EXT2 interface to the INT2 interface.	Internal -> External	custom or ANY

Table 4: FortiBridge probes and FortiGate firewall policy requirements (Continued)

Probe	Description	FortiGate Firewall policy	
		Direction	Service
mm7	MM7 packets are sent from the INT2 interface to the EXT2 interface, through the FortiGate unit. When the packet is received, an MM7 response is sent back from the EXT2 interface to the INT2 interface.	Internal -> External	custom or ANY

*No predefined service selections are offered for the MMS protocols. To allow the probes for these protocols, you can select the ANY service or create custom services for TCP packets with the destination ports listed in *Probe > Settings*.

Enabling probes to detect FortiGate hardware failure

A FortiGate unit can stop processing network traffic because of a hardware failure such as the failure of a hardware component, a loss of power, or a loss of connectivity if a network cable is unplugged.

If a hardware failure occurs, the FortiGate unit stops processing all traffic. You can enable any FortiBridge probe for the FortiBridge unit to detect a FortiGate hardware failure.

Enabling probes to detect FortiGate software failure

A FortiGate unit can also stop processing network traffic because of a software failure. For example, a firmware issue could cause a specific software process to crash. Also, network traffic could increase to a point where the FortiGate unit cannot process all traffic. As a result, the FortiGate unit could stop processing some or all traffic without a hardware failure occurring.

To detect a FortiGate software failure, you can enable probes for FortiGate services that you want to provide fail open protection for. For example, if SMTP email services are a high priority for your network, you should enable the SMTP probe. If the SMTP probe detects a failure of SMTP traffic through the FortiGate unit, the FortiBridge unit switches to bypass mode to maintain SMTP traffic flow.

If you do not consider FTP traffic a high priority, you can leave the FTP probe disabled. In this configuration, if only FTP traffic fails, the FortiBridge does not switch to bypass mode.

Probe interval and probe threshold

For each probe, you set a probe interval and a probe threshold. The probe interval defines how often to test the connection. The probe threshold defines how many consecutive failed probes can occur before the FortiBridge considers the connection to have failed.

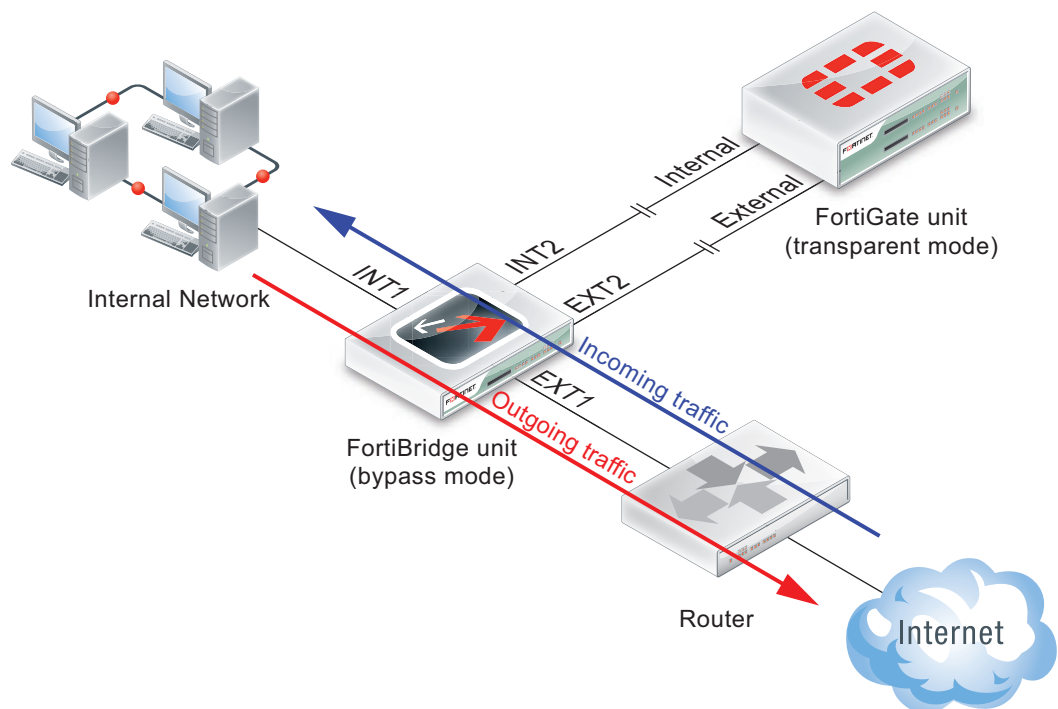
Bypass mode operation

When the FortiBridge unit operates in bypass mode, the FortiBridge INT1 and EXT1 interfaces are directly connected. All traffic between the internal and external network segments flows, whether or not the FortiGate unit is operating normally.

Because the INT1 and EXT1 interfaces are directly connected, you cannot use Telnet or SSH to connect to the FortiBridge CLI. Instead you must use a console connection.

The FortiBridge unit remains in bypass mode even if the FortiGate unit recovers. To restore the FortiGate unit, you must manually switch the FortiBridge unit back to normal mode. You can switch the FortiBridge unit to normal mode by pressing the mode switch on the FortiBridge front panel or by using a console connection to the CLI and entering the command `execute switch-mode`. You can also use the mode switch and the `execute switch-mode` command to manually switch the FortiBridge unit from normal mode to bypass mode.

Figure 32: FortiBridge unit operating in bypass mode



When the FortiBridge unit is operating in bypass mode you can still connect to the FortiBridge CLI and manage the FortiBridge unit (for example to switch the FortiBridge unit to normal mode). When the FortiBridge unit operates in bypass mode, you cannot connect to the FortiGate interfaces that are connected to the FortiBridge unit.

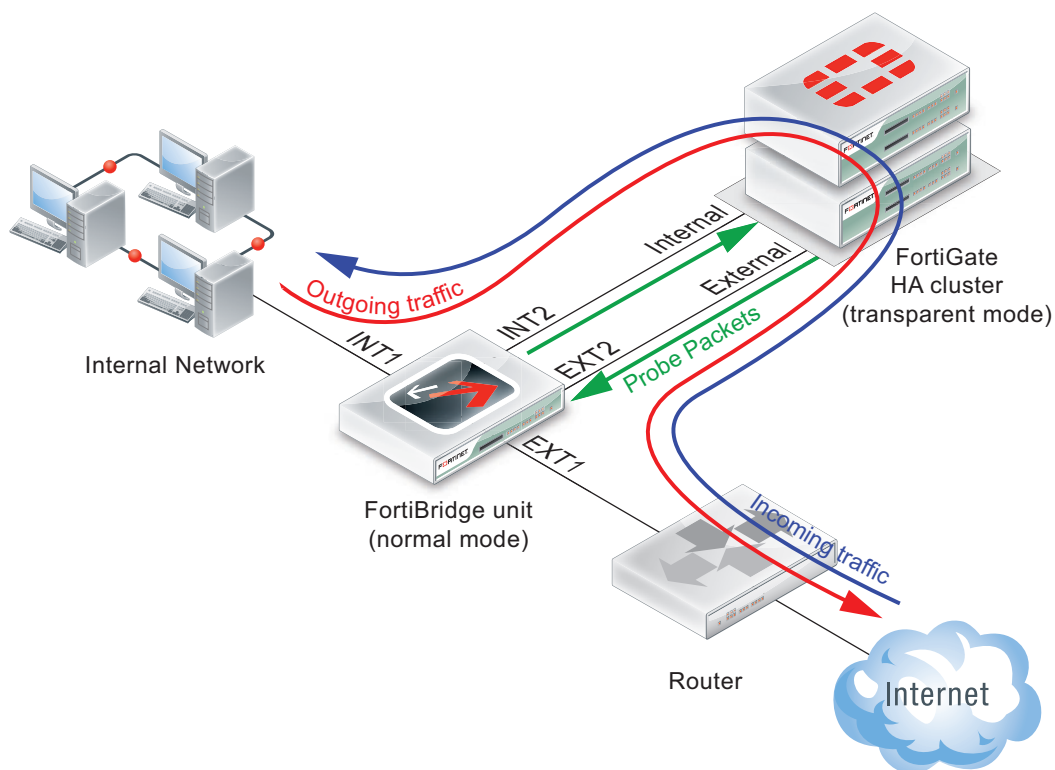
FortiBridge power failure

If a power failure occurs and the FortiBridge unit loses power, zero power fail-open technology causes FortiBridge unit to fail open. The FortiBridge unit bypasses the FortiGate unit and all traffic passes between the FortiBridge INT1 and EXT1 interfaces. If power is restored to the FortiBridge unit, it starts up in bypass mode and then switches to normal mode when its start up sequence is complete, reconnecting the FortiGate unit to the network.

Example FortiGate HA cluster FortiBridge application

A FortiBridge unit can provide fail open protection for a FortiGate HA cluster operating in transparent mode in much the same way as for a standalone FortiGate unit. To provide fail open protection for an HA cluster, connect the FortiBridge unit to the switches that connect the internal and external interfaces of the cluster. Use the following steps to connect a FortiBridge unit to the HA cluster, as shown in Figure 33:

Figure 33: FortiBridge unit providing fail open protection for a FortiGate HA cluster



The network configuration and FortiBridge configuration are the same for a cluster and for a standalone FortiGate unit. In normal mode, packets pass through the FortiBridge unit and through the FortiGate HA cluster and back through the FortiBridge unit. For the cluster to process this traffic, you must add Internal -> External firewall policies to the cluster configuration. If a failure occurs and the cluster no longer processes traffic, the FortiBridge unit switches to bypass mode, bypassing the cluster.

The connection procedure is different depending on whether the FortiBridge unit uses copper gigabit ethernet network connections or fiber gigabit ethernet network connections. This section includes the following connection procedures:

- [Connecting the FortiBridge-2002 \(copper gigabit ethernet\)](#)
- [Connecting the FortiBridge-2002F \(fiber gigabit ethernet\)](#)

Connecting the FortiBridge-2002 (copper gigabit ethernet)

The FortiBridge-2002 unit contains 4 auto-sensing 10/100/1000 Ethernet interfaces that connect to the internal and external networks and to the cluster interfaces that were connected to these networks. Use the following steps to connect a FortiBridge-2002 unit to the network as shown in [Figure 33](#).



Normally, you would use straight-through ethernet cables to connect the FortiBridge-2002 unit to the FortiGate unit and to your networks. However, for some connections you may need a crossover ethernet cable (for example, for compatibility with network devices that do not support Auto MDI/MDIX).

- 1 Connect the FortiBridge-2002 INT2 interface to the switch connected to the HA cluster internal interface.
- 2 Connect the switch connected to the HA cluster external interface to the FortiBridge-2002 EXT2 interface.
- 3 Connect the internal network to the FortiBridge-2002 INT1 interface.
- 4 Connect the FortiBridge-2002 EXT1 interface to the router.

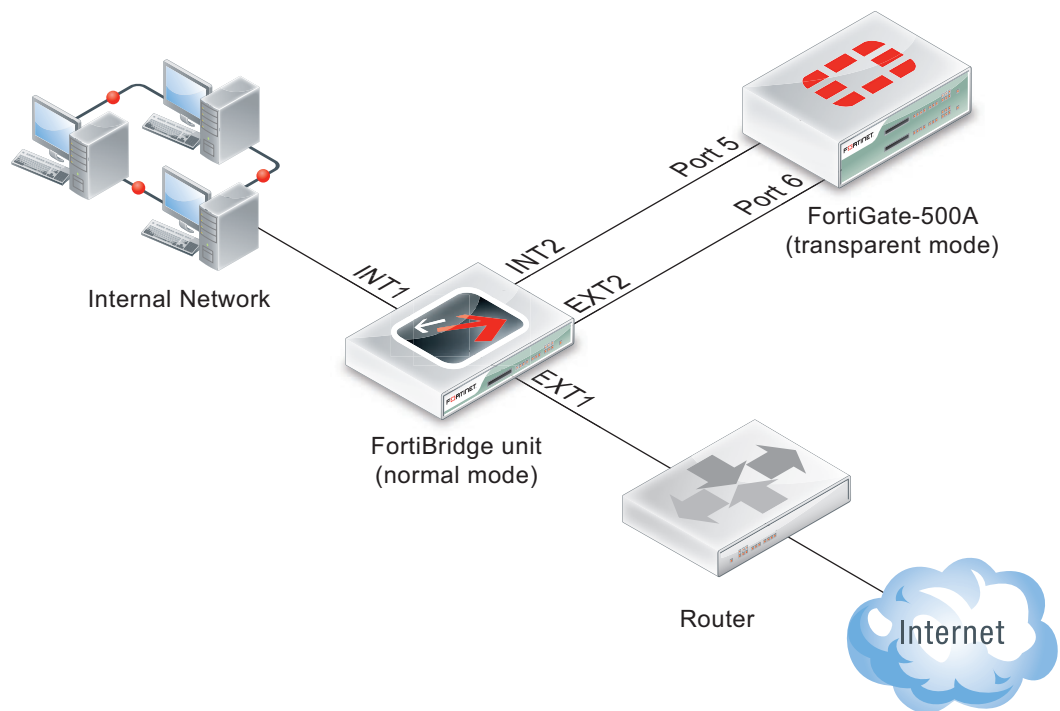
Connecting the FortiBridge-2002F (fiber gigabit ethernet)

The FortiBridge-2002F unit contains 4 multimode fiber optic gigabit interfaces that connect to the internal and external networks and to the FortiGate cluster interfaces that were connected to these networks. Use the following steps to connect a FortiBridge-2002F unit to the network as shown in [Figure 29](#).

- 1 Connect the FortiBridge-2002F INT2 interface to the switch connected to the HA cluster internal interface.
- 2 Connect the switch connected to the HA cluster external interface to the FortiBridge-2002F EXT2 interface.
- 3 Connect the internal network to the FortiBridge-2002F INT1 interface.
- 4 Connect the FortiBridge-2002F EXT1 interface to the router.

Example configuration with other FortiGate interfaces

All of the examples in this chapter describe using the FortiBridge unit to provide fail open protection for traffic passing between the FortiGate unit internal and external interfaces. You can actually use a FortiBridge unit to provide fail open protection for any two FortiGate unit interfaces. No limitation is implied by naming the FortiBridge interfaces INT and EXT. These names are used to simplify installation procedures. [Figure 34](#) shows a FortiBridge unit providing fail open protection for network traffic between ports 5 and 6 of a FortiGate-500A unit.

Figure 34: FortiBridge unit providing fail open protection for a single FortiGate unit

To connect a FortiBridge unit to the network shown in [Figure 34](#):

- 1 Connect the FortiBridge INT2 interface to the FortiGate-500A port 5 interface.
- 2 Connect the FortiGate-500A port 6 interface to the FortiBridge EXT2 interface.
- 3 Connect the internal network to the FortiBridge INT1 interface.
- 4 Connect the FortiBridge EXT1 interface to the router.

You must add port 5 -> port 6 firewall policies to the FortiGate-500A unit configuration.

Completing the basic FortiBridge configuration

Now that you have connected the FortiBridge unit to your network and connected to the FortiBridge CLI, use the following procedures to complete the basic configuration of the FortiBridge unit.



Not all of the following procedures are required to complete the basic FortiBridge unit configuration. Choose the procedures that apply to your installation.

- [Adding an administrator password](#)
- [Changing the management IP address](#)
- [Changing DNS server IP addresses](#)
- [Changing the default gateway and adding static routes](#)
- [Allowing management access to the EXT1 interface](#)
- [Changing the system time and date](#)
- [Adding administrator accounts](#)

When you complete the procedures in this chapter, the FortiBridge unit will be operating and connected to your network and to your FortiGate unit. See [“Example network configuration” on page 79](#) to configure the FortiBridge unit to monitor the status of the FortiGate unit and to fail open if the FortiBridge unit detects that the FortiGate unit has failed.

Adding an administrator password

Add an administrator password to the default admin administrator account to prevent unauthorized users from connecting to and managing the FortiBridge unit.

To add an administrator password — Web-based manager

- 1 Go to *System > Status*.
- 2 In the Administrators section of the dashboard, select the *Edit* icon of the admin user.
- 3 Select the *Change Password* link.
- 4 Enter the new password.
- 5 Enter the new password again in the second field.
- 6 Select *OK*.

To add an administrator password — CLI

```
config system admin
  edit admin
    set password <password_str>
  end
```

Changing the management IP address

Change the FortiBridge unit management IP address so that you can connect to the FortiBridge CLI from your network (instead of being required to use a direct console connection). The management IP should be a valid IP address for your network.

To change the management IP address — Web-based manager

- 1 Go to *System > Status*.
- 2 Select the *Change* link in the Management Port section of the dashboard.
- 3 Enter the new management IP address and netmask in the IP/Netmask field.
- 4 Select *OK*.

To change the management IP address — CLI

```
config system manageip
    set ip <management_ipv4mask>
end
```

Changing DNS server IP addresses

Change the FortiBridge DNS server IP addresses to the IP addresses of your DNS servers. The correct DNS server configuration is required for alert email.

To change DNS server IP addresses — Web-based manager

- 1 Go to *System > Status*.
- 2 Select the *Change* link in the Management Port section of the dashboard.
- 3 Enter the primary DNS IP address in the *Primary DNS Server* field.
- 4 Enter the secondary DNS IP address in the *Secondary DNS Server* field.
- 5 Select *OK*.

To change DNS server IP addresses — CLI

```
config system dns
    set primary <primary_ipv4>
    set secondary <secondary_ipv4>
end
```

Changing the default gateway and adding static routes

Add static routes if you need to route packets from the FortiBridge unit through a router to another network. For example, if alert email sends email messages from the internal network to an email server on the Internet, you should add a route to the Internet.

The web-based manager allows you to enter only the default gateway. If you require additional static routes, use the CLI to enter them.

To change the default gateway — Web-based manager

- 1 Go to *System > Status*.
- 2 Select the *Change* link in the Management Port section of the dashboard.
- 3 Enter the default gateway IP address in the *Default Gateway* field.

To change the default gateway — CLI

```
config system route
    edit <sequence_int>
        set gateway <gateway_ipv4>
    end
```

To add additional static routes — CLI

```
config system route
```

```

edit <sequence_int>
  set gateway <gateway_ipv4>
  set dst <destination_ipv4mask>
end

```

Allowing management access to the EXT1 interface

By default no management access is configured for the EXT1 interface. Use the following procedure to add management access to this interface if required.

Configuring the EXT1 interface to allow management access is possible only using the CLI.

To allow management access to the EXT1 interface — CLI

```

config system interface external
  set allowaccess ssh
end

```

Changing the system time and date

Use the following procedure to change the system time and date.

To change the system time and date — Web-based manager

- 1 Go to *System > Status*.
- 2 Select the *Change* link beside *System Time* in the System Information section of the dashboard.
- 3 Enter the time, date, and timezone as required.
- 4 Select *OK*.

To change the system time and date — CLI

```

execute time <hh:mm:ss>
execute date <mm/dd/yyyy>
config system global
  set timezone <timezone_int>
end

```

Enter the number corresponding to your time zone. Type ? to list time zones and their numbers.

For example, to set the time zone to Central time (time zone number 8), enter:

```

config system global
  set timezone 8
end

```

For information about configuring other global settings, see “system global” in the [FortiBridge CLI Reference](#).

Adding administrator accounts

The factory default FortiBridge configuration includes the admin administrator account. Use this procedure to add more administrator accounts.

To add administrator accounts — Web-based manager

- 1 Go to *System > Status*.
- 2 In the Administrators section of the dashboard, select *Create New*.

- 3 Enter the administrator account name.
- 4 Enter the administrator account password.
- 5 Enter the password again in the second field.
- 6 Select *OK*.

To add administrator accounts — CLI

```
config system admin
  edit <admin_name_str>
    set password <password_str>
    set accprofile prof_admin
  end
```

For more information about configuring administrators see “system admin” in the [FortiBridge CLI Reference](#).

Resetting to the factory default configuration

Use the following procedure to reset the FortiBridge unit to the factory default configuration. You might want to reset the FortiBridge to the factory default condition if the FortiBridge unit is not functioning as expected and you would like to re-start the configuration process. Resetting to the factory default configuration resets all configuration changes that you have made, including the management IP address.

To reset to factory default configuration from the FortiBridge front panel

- 1 Use a pen or other pointed object to press the Factory reset button.
After a few seconds the FortiBridge unit restarts; reset to the factory default configuration. You can now re-configure the FortiBridge unit.

To reset to factory defaults — CLI

```
execute factoryreset
```

A few seconds after confirming your command, the FortiBridge unit restarts, reset to the factory default configuration. You can now re-configure the FortiBridge unit.

Installing FortiBridge unit firmware

Before beginning any of the procedures in this section, you must have the FortiBridge firmware image file that you are going to install on the FortiBridge unit. During these procedures you are required to enter the name of the firmware image file.

Changing firmware versions

You can use these procedure to upgrade to a newer version of the FortiBridge firmware, re-install the current version, or revert to an older version of the firmware.

The CLI-based procedure requires that you have a TFTP server you can connect to from the FortiBridge unit.

Changing firmware versions — Web-based manager

- 1 Go to *System > Status*.
- 2 In the System Information section, the Firmware Version displays the currently installed firmware version.

- 3 Select *Update* to install another version of the firmware.
- 4 Select *Browse* to choose the firmware file on your computer.
- 5 Select *OK* to install the firmware file.
- 6 If you are installing an older version of the firmware, you must confirm your selection before the installation can proceed.
- 7 The FortiBridge installs the firmware and restarts. This process takes a few minutes.
- 8 To confirm that the firmware you selected is installed, log into the web-based manager, go to *System > Status*, and confirm that the firmware version is correct.

Changing firmware versions — CLI

- 1 Make sure that the TFTP server is running.
- 2 Copy the new firmware image file to the root directory of your TFTP server.
- 3 Log into the CLI as an administrator with `sys shutdown ngrp` access.
Normally this would be the admin administrator. But you can use access profiles to control administrative access. See “system accprofile” in the [FortiBridge CLI Reference](#) for more information.
- 4 Make sure the FortiBridge unit can connect to the TFTP server.
You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiBridge unit:

```
execute restore image <name_str> <tftp_ip>
```

Where `<name_str>` is the name of the firmware image file on the TFTP server and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `FBG_2002-v30-build010-FORTINET.out` and the IP address of the TFTP server is 192.168.1.23, enter:

```
execute restore image FBG_2002-v30-build010-FORTINET.out
192.168.1.168
```

- 6 If you are downgrading to an older firmware version, a message is displayed:
Get image from tftp server OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
If you are certain that you want to downgrade to the older firmware version, press `Y`.
- 7 The FortiBridge installs the firmware and restarts. This process takes a few minutes.
- 8 Reconnect to the CLI.
- 9 To confirm that the new firmware image has been loaded, enter:

```
get system status
```

Installing firmware from a system reboot

This procedure installs a specified firmware image and resets the FortiBridge unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or to re-install the current firmware.

To use this procedure you:

- access the CLI by connecting to the FortiBridge console port,

- install a TFTP server that you can connect to from the FortiBridge EXT2 interface. The TFTP server should be on the same network as the EXT2 interface. The FortiBridge unit cannot access the TFTP server if its behind a router.

During this procedure you will be asked to enter a local IP address for the FortiBridge unit. This is a temporary address used for downloading the firmware image.

This procedure reverts your FortiBridge unit to its factory default configuration. Before running this procedure you can backup the FortiBridge unit configuration using the command `execute backup config`.

To install firmware from a system reboot

- 1 Connect to the CLI using the FortiBridge console port.
- 2 Make sure the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of the TFTP server.
- 4 Make sure the EXT2 interface of the FortiBridge unit can connect to the TFTP server.
- 5 Enter the following command to restart the FortiBridge unit:

```
execute reboot
```

As the FortiBridge unit starts, a series of system startup messages are displayed. When the following messages appears:

```
Hit any key to stop autoboot:
```

- 6 Immediately press any key to interrupt the system startup.



You only have 3 seconds to press any key. If you do not press any key soon enough, the FortiBridge unit reboots and you must log in and repeat the `execute reboot` command.

When you successfully interrupt the startup process, the `=>` prompt appears:

- 7 Type `upgrade` and press Enter to get the new firmware image from the TFTP server. The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

- 8 Type the address of the TFTP server and press Enter.

The following message appears:

```
Enter local address [192.168.1.188]:
```

- 9 Type an IP address that the FortiBridge unit can use to connect to the TFTP server press Enter.



The local IP address is a temporary address used to download the firmware image. The local IP address should be on the same subnet as the TFTP server IP address.

The following message appears:

```
Enter firmware image file [image.out]:
```

- 10 Type the firmware image file name and press Enter.

The TFTP server uploads the firmware image file to the FortiBridge unit and the FortiBridge unit installs the new firmware image, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

- 11 Reconnect to the CLI.

12 To confirm that the firmware image has been loaded, enter:

```
get system status
```


Example network configuration

This chapter describes how to configure a FortiBridge unit to provide fail open protection for a FortiGate unit operating in transparent mode. This chapter also describes some commonly required FortiBridge operating procedures such as recovering from a fail open event, manually switching between FortiBridge operating modes and backing up and restoring the FortiBridge configuration.

The procedures in this chapter assume that you have connected the FortiBridge unit to your network and completed its basic configuration as described in [“Completing the basic FortiBridge configuration” on page 71](#).



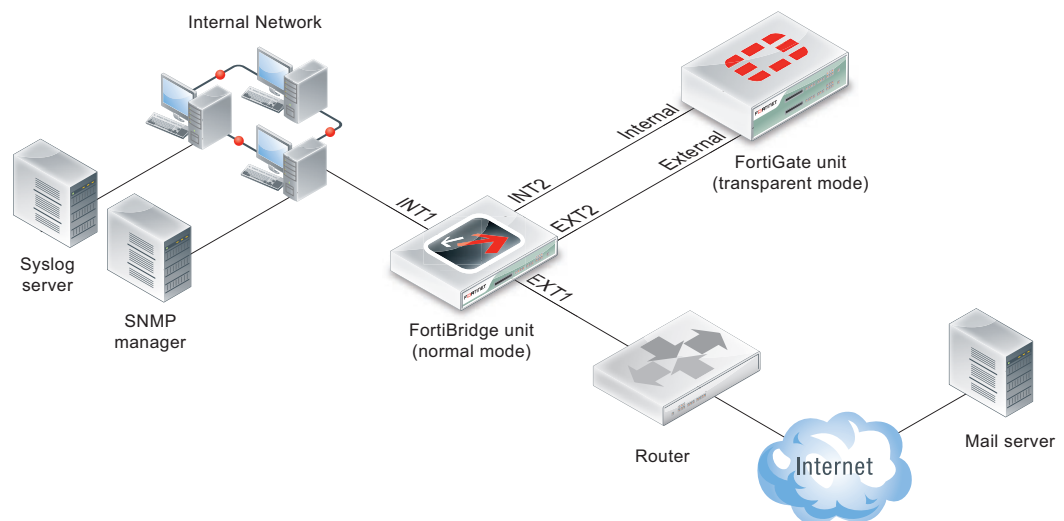
The information in this chapter can be applied to any standalone FortiGate transparent mode network configuration. These procedures can also be applied to a FortiBridge unit providing fail open protection for a FortiGate HA cluster operating in transparent mode.

The descriptions and procedures in this section assume that the FortiGate unit is installed between an internal network and the router that connects the internal network to the Internet as show in [Figure 35](#). The FortiGate unit can provide the following security services for all traffic passing between the internal network and the internet:

- Internal -> External firewall policies for HTTP, FTP, POP3, SMTP, and IMAP connections from Internal network to the Internet.
- Virus scanning of HTTP, FTP, POP3, SMTP, and IMAP traffic,
- Web filtering of HTTP traffic,
- Spam filtering of POP3, SMTP, and IMAP traffic.

In addition to the above security services, a FortiCarrier unit can process MM1, MM3, MM4, and MM7 traffic.

Figure 35: Example FortiBridge application



[Table 5](#) lists the internal network configuration.

Table 5: Internal network configuration

FortiGate management IP address	172.20.120.10/24
Internal network subnet IP address	172.20.120.0/24

Table 5: Internal network configuration (Continued)

Router internal IP address	172.20.120.1/24
Internal network default route	172.20.120.1
Primary DNS server	172.20.120.2
Secondary DNS server	172.20.120.3
Syslog Server IP address	172.20.120.11
SNMP Manager IP address	172.20.120.12
Mail Server Name	mail.myorg.com

[Table 6](#) lists the basic FortiBridge unit configuration settings.

Table 6: Basic FortiBridge unit configurations settings

Administrator password	passWORD
Management IP address	172.20.120.20/24
Default route	172.20.120.1
Primary DNS server	172.20.120.2
Secondary DNS server	172.20.120.3

Configuring FortiBridge probes

To monitor a FortiGate unit for failure, you configure the FortiBridge unit to send probe packets through the FortiGate unit. Using probe packets, the FortiBridge unit can confirm that the FortiGate unit can process ICMP (ping), HTTP, FTP, POP3, SMTP, IMAP, MM1, MM3, MM4, and MM7 traffic. Until you configure probes, the FortiBridge unit cannot detect if the FortiGate unit has failed.

This section describes:

- [Probe settings](#)
- [Enabling probes](#)
- [Verifying that probes are functioning](#)
- [Tuning the failure threshold and probe interval](#)

Probe settings

Configure probe settings to control the response when a FortiBridge probe detects that the FortiGate unit has failed. Probe settings consist of:

Table 7: Probe settings

Probe Setting	Description	Default
Action on failure	Set the FortiBridge unit response when a probe detects that the FortiGate unit has failed. The FortiBridge unit can, • Send alertmail • Fail open • Send an SNMP trap • Send a message to a syslog server You can add up to four actions on failure. All of the configured actions on failure occur when the FortiBridge unit detects a failure.	fail open
Dynamic IP pattern	Configure the INT2 and EXT2 interfaces with dynamic probe IP addresses. The dynamic probe IP addresses should not conflict with IP addresses on the network that the FortiGate unit is connected to. These IP addresses are not visible from the outside network, but they should not conflict with IP addresses in packets passing through the FortiBridge unit. You cannot change the dynamic IP pattern if any probes are enabled.	(none)
FortiGate unit serial number	The serial number of the FortiGate unit that the FortiBridge unit is connected to. The serial number appears in FortiBridge alert mail, and syslog messages to identify the FortiGate unit.	(none)

To configure probe settings

This procedure shows how to configure the following probe settings:

- The FortiBridge unit responds to a FortiGate unit failure by failing open and by sending an alert email, a syslog message, and an SNMP trap
- The dynamic IP pattern is 2.2.2.*
- The FortiGate unit serial number is FGT8002803923050



The FortiBridge unit does not have to fail open if the FortiGate unit fails. The FortiBridge unit can be configured just to send alerts if the FortiGate unit fails.

Configure probe settings — Web-based manager

- 1 Go to *Probe > Settings*.
- 2 Enter the IP pattern in the *Probe IP Address Pattern* field.
- 3 Select *Apply*.
- 4 Go to *Probe > Notifications*.

5 Select the notification types you require.

6 Select *Apply*.

You cannot set the failopen or failcutoff action, nor the FortiGate serial number using the web-based manager.

Configure probe settings — CLI

```
config probe setting
  set action_on_failure alertmail failopen snmp syslog
  set dynamic_ip_pattern 2.2.2.*
  set fgt_serial FGT8002803923050
end
```

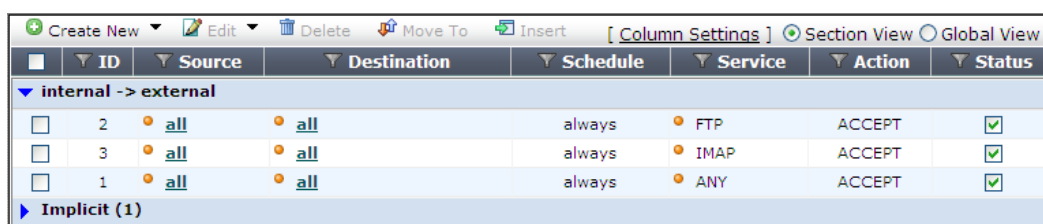
Enabling probes

Enable probes to control the protocols that the FortiBridge unit uses to confirm that the FortiGate unit is functioning normally. You can configure probes for ping (ICMP), HTTP, FTP, POP3, SMTP, IMAP, MM1, MM3, MM4, and MM7 protocols. For all probes you can configure the probe interval (the time between consecutive probe packets) and the probe threshold (the number of probe packets lost before the FortiBridge unit registers a failure). For HTTP, FTP, POP3, SMTP, and IMAP probes you can also change the probe port. You would change the probe port for a protocol if the FortiGate unit uses a non-standard port for that protocol.

The FortiBridge unit simultaneously tests connectivity through the FortiGate unit for each probe that you have enabled. The first probe that registers a failure causes all probes to stop and the configured action on failure to occur.

Before you configure probes, the FortiGate unit must be configured to pass the probe traffic. A single Internal->External firewall policy that allows all traffic also allows all probe packets. You can also configure individual policies for each protocol. For example, you could add the firewall policies shown in [Figure 36](#) to the FortiGate unit.

Figure 36: Sample firewall policies



ID	Source	Destination	Schedule	Service	Action	Status
2	all	all	always	FTP	ACCEPT	☒
3	all	all	always	IMAP	ACCEPT	☒
1	all	all	always	ANY	ACCEPT	☒

Policy 1 processes any network traffic. Policy 2 processes all FTP traffic. Policy 2 is above Policy 1 in the policy list, so FTP traffic is matched by policy 2. In the same way, Policy 3 processes all IMAP traffic.

FTP and IMAP probes would be processed by policies 2 and 3 respectively. All other probes would be processed by policy 1. This would include pings, SMTP traffic and so on.

To enable and configure FortiBridge probes — Web-based manager

The following steps show examples for configuring ping, HTTP, FTP, POP3, SMTP, and IMAP probes. For a complete description of FortiBridge probes see “probe probe_list {ping | http | ftp | pop3 | smtp | imap | mm1 | mm3 | mm4 | mm7}” in the [FortiBridge CLI Reference](#).

1 Go to *Probe > Settings*.

- 2 For the ping protocol, select *Enable*.
This enables ping probes with the default settings.
- 3 For the FTP protocol, select *Enable*, enter 5 for the *Interval*, and enter 8 for the *Failure-Threshold*.
These settings have the FortiBridge unit send an FTP probe every 5 seconds and fail open if 8 consecutive FTP probe packets are not received.
- 4 For the IMAP protocol, select *Enable*.
This enables IMAP probes with the default settings.
- 5 For the SMTP protocol, select *Enable* and enter 26 for the *Port Number*.
This enables SMTP probes on port 26.

To enable and configure FortiBridge probes — CLI

- 1 Enable the ping probe using the default ping probe parameters. Enter:


```
config probe probe_list ping
    set status enable
end
```
- 2 Display ping probe settings, enter:


```
get probe probe_list ping
    name           : ping
    failure_threshold : 3
    probe_interval  : 1
    status          : enable
```
- 3 Enable the FTP probe. Increase the failure threshold to 5 and the probe interval to 8.


```
config probe probe_list ftp
    set status enable
    set failure_threshold 8
    set probe_interval 5
end
```

The FortiBridge unit sends an FTP probe every 5 seconds and fails open if 8 consecutive FTP probe packets are not received.
- 4 Display FTP probe settings. Enter:


```
get probe probe_list ftp
    name           : ftp
    failure_threshold : 8
    probe_interval  : 5
    status          : enable
    test_port       : 21
```
- 5 Enable the IMAP probe. Enter:


```
config probe probe_list IMAP
    set status enable
end
```
- 6 Enable the SMTP probe and change the port used by the probe from 25 to 26. Enter:


```
config probe probe_list SMTP
    set status enable
    set test_port 26
end
```

Verifying that probes are functioning

You verify that the probes are functioning by viewing the sessions being processed by the FortiGate unit.

To verify that probes are functioning

- 1 Go to *System > Dashboard > Status*.
- 2 In the Top Sessions widget, select *Details* at the bottom of the widget.
The current sessions list appears. Optionally select *Detach* to detach and expand the browser window to see the entire list.
- 3 View the sessions on the *Session* list.

Figure 37: FortiGate Session list showing FortiBridge probes

1 / 1 Total: 4 Clear All Filters Return									
#	Protocol	Source Address	Source Port	Destination Address	Destination Port	Policy ID	Expiry (sec)	Duration (sec)	
1	tcp	2.2.2.13	1053	2.2.2.14	143	3	3352	4486	
2	tcp	2.2.2.13	1054	2.2.2.14	21	2	3600	4486	
3	icmp	2.2.2.13		2.2.2.14		1	3598	28	
4	tcp	2.2.2.13	1052	2.2.2.14	26	1	3598	4486	

This session list shows the following:

- The FortiBridge dynamic probe IP addresses are 2.2.2.213 and 2.2.2.214.
- IMAP probe packets (port 143) are processed by firewall policy 3.
- FTP probe packets (port 21) are processed by firewall policy 2.
- ping probe packets are processed by firewall policy 1.
- SMTP packets using port 26 are processed by firewall policy 1.

Tuning the failure threshold and probe interval

If you find the FortiBridge unit failing open when the FortiGate unit has not failed or if the FortiGate unit fails and there is an unacceptably long delay before the FortiBridge unit fails open, you should adjust the failure threshold and probe interval.

Failing open when the FortiGate unit has not failed indicates that you should increase the time the FortiBridge unit waits to fail open. During startup, if the FortiBridge unit begins sending probe packets before the FortiGate unit has completed its start up sequence the FortiBridge unit may detect a failure and switch to bypass mode. Also, if the FortiGate unit is processing high traffic volumes, a fail open could occur if the FortiGate unit delays FortiBridge probe packets. You can increase the fail open delay by increasing the failure threshold and probe interval.

An unacceptable delay before failing open means network traffic can be interrupted for the time period between when the FortiGate unit fails and the FortiBridge unit fails open. You can minimize the delay by reducing the failure threshold and probe interval.

Configuring FortiBridge alerts

Configure FortiBridge alerts so that the `alertemail`, `syslog`, and `snmp` actions on failure cause the FortiBridge unit to notify system administrators that the FortiGate unit has failed. Until you configure alert email, syslog, and SNMP alerts, the FortiBridge cannot notify system administrators of a FortiGate failure.

You can configure the following FortiBridge alerts:

- [FortiBridge alert email](#)

- [FortiBridge syslog](#)
- [FortiBridge SNMP](#)

FortiBridge alert email

If you set the probe action on failure to `alertmail`, you can configure alert email so that the FortiBridge unit sends an email message to up to three email addresses if the FortiBridge unit detects a failure. The alert email informs the recipient that a FortiGate unit has failed, includes the protocol for which the failure was detected, and includes the serial number of the FortiGate unit that failed.

Only the first probe to detect a failure triggers the actions on failure. So, even if multiple probes are configured, when a failure is detected, the FortiBridge unit sends one alert email.

Figure 38: Sample FortiBridge alert email message

```
FortiBridge detect FortiGate failure

Time: Tue Feb  1 19:58:46 2010
failed protocol: http
failed FortiGate serial number: FGT8002803923050
```

To configure alert email — Web-based manager

Configuring FortiBridge alert email is similar to configuring FortiGate alert email.

- 1 Go to *Probe > Notifications*.
- 2 Enable *Email*.
- 3 Enter your email server name in the *SMTP Server* field.
- 4 Enter the email addresses to which the alert email messages are sent in the *Email to* fields. Three fields are provided for up to three addresses.
- 5 If your email server requires authentication to send messages, select *Authentication* and enter your SMTP user name and password.
- 6 Select *Apply*.

To configure alert email — CLI

```
config alertemail setting
    set server mail.myorg.com
    set username user@company.com
    set password PassWORD
    set mailto1 user@company.com
    set mailto1 user2@company.co.uk
    set mailto1 user3@company.com
end
```

FortiBridge syslog

If you set the probe action on failure to `syslog`, you can configure the FortiBridge unit to send a syslog message to one syslog server if the FortiBridge unit detects a failure. The message informs the recipient that a FortiGate unit has failed, includes the protocol for which the failure was detected, and includes the serial number of the FortiGate unit that failed.

Only the first probe to detect a failure triggers the actions on failure. So, even if multiple probes are configured, when a failure is detected, the FortiBridge unit sends one message.

Figure 39: Sample FortiBridge syslog messages

```
02-01-2010 18:22:50 Local7.Alert 172.20.120.13 date=2010-02-01
time=15:28:22 device_id= log_id=0100020001 type=event
subtype=system pri=alert msg="FortiBridge detect FortiGate
failure: [failed time: Tue Feb 1 15:28:22 2010][failed protocol:
http] [failed FortiGate serial number: FGT8002803923050]"
02-01-2010 8:21:27 Local7.Alert 172.20.120.13 date=2010-02-01
time=15:26:59 device_id= log_id=0100020001 type=event
subtype=system pri=alert msg="FortiBridge detect FortiGate
failure: [failed time: Tue Feb 1 15:26:59 2010][failed protocol:
ftp] [failed FortiGate serial number: FGT8002803923050]"
02-01-2010 18:17:17 Local7.Alert 172.20.120.13 date=2010-02-01
time=15:22:49 device_id= log_id=0100020001 type=event
subtype=system pri=alert msg="FortiBridge detect FortiGate
failure: [failed time: Tue Feb 1 15:22:49 2010][failed protocol:
ping] [failed FortiGate serial number: FGT8002803923050]"
02-01-2010 8:13:43 Local7.Alert 172.20.120.13 date=2010-02-01
time=15:19:15 device_id= log_id=0100020001 type=event
subtype=system pri=alert msg="FortiBridge detect FortiGate
failure: [failed time: Tue Feb 1 15:19:15 2010][failed protocol:
smtp] [failed FortiGate serial number: FGT8002803923050]"
```

To configure FortiBridge syslog — Web-based manager

In most cases you should only need to configure the IP address of the syslog server to receive FortiBridge syslog messages. See “log syslogd setting” in the [FortiBridge CLI Reference](#) for more FortiBridge syslog options.

- 1 Go to *Probe > Notifications*.
- 2 Enable *Syslog*.
- 3 In the IP address field, enter the syslog server address
- 4 If required, configure the port, facility, and format.
- 5 Select *Apply*.

To configure FortiBridge syslog — CLI

```
config log syslogd setting
    set server 172.20.120.11
end
```

FortiBridge SNMP

If you set the probe action on failure to `snmp`, you can configure FortiBridge SNMP settings so that the FortiBridge unit sends SNMP v1 and v2c compliant traps to SNMP v1 and v2c compliant SNMP managers if the FortiBridge unit detects a failure. The traps inform the recipient that a FortiGate unit has failed and include the protocol for which the failure was detected.

Only the first probe to detect a failure triggers the actions on failure. So, even if multiple probes are configured, when a failure is detected, the FortiBridge unit sends one v1 SNMP trap and one v2c SNMP trap.

Configure FortiBridge SNMP by adding and configuring an SNMP community. An SNMP community is a grouping of equipment for network administration purposes. You can add up to three SNMP communities. Each community can have a different configuration for SNMP traps. You can add the IP addresses of up to 8 SNMP managers to each community.

To add and enable an SNMP community — Web-based manager

- 1 Go to *Probe > Notifications*.
- 2 Enable *SNMP*.
- 3 In the *Community Name* field, enter an SNMP community name.
- 4 Enter the address of an SNMP manager in the *IP Address* field.
You may enter up to eight SNMP manager addresses.
- 5 Select *Apply*.

To add and enable an SNMP community — CLI

```
config system snmp community
  edit 1
    set name snmp_1
  end
```

The new SNMP community, named snmp1, is enabled by default. SNMP v1 and v2 traps are also enable by default. You can disable traps and change ports. See “[system snmp community](#)” in the *FortiBridge CLI Reference* for more information.

Add the IP addresses of two SNMP managers that can receive traps.

```
config system snmp community
  edit 1
    config hosts
      edit 1
        set ip 172.20.120.12
      next
      edit 2
        set ip 192.168.20.102
      end
    end
  end
```

Recovering from a FortiGate failure

After a FortiBridge probe detects a FortiGate failure, the FortiBridge unit stops sending probes. To restart probes you can restart the FortiBridge unit, connect to the FortiBridge CLI and enter the `execute switch-mode` command, or press the mode button on the FortiBridge unit front panel.

Normally, an action on failure causes the FortiBridge unit to fail open. When the FortiBridge unit fails open, it begins operating in Bypass mode. In bypass mode the INT1 and EXT1 interfaces are directly connected and you cannot use Telnet or SSH to connect to the FortiBridge CLI. Use the following procedure to recover from bypass mode after a FortiGate failure and resume normal operation.

To resume normal operation from bypass mode

When the FortiBridge unit is operating in bypass mode, you need to do the following to resume normal operation:

- 1 Review FortiBridge alerts and check the status of your FortiGate unit and network components to determine the source of the failure.

A network component or the FortiGate unit could have experienced a general hardware failure or a specific software failure.

- 2 Make the required changes to fix the problem.

Depending on the cause, this could mean re-connecting and restarting the FortiGate unit, or diagnosing a problem with the FortiGate unit or other network component.

If all network and FortiGate unit hardware and software is functioning normally, you may have to adjust FortiBridge probe settings. See [“Tuning the failure threshold and probe interval” on page 84](#).

- 3 Manually switch the FortiBridge unit from bypass to normal mode.

Connect to the FortiBridge CLI using the console connection and enter the command:

```
execute switch-mode
```

Or press the Mode button on the FortiBridge unit front panel.

Or restart the FortiBridge unit by cycling the power or from the console using the `execute reboot` command. The FortiBridge unit always restarts in normal mode.

Manually switching between FortiBridge operating modes

You can manually switch between FortiBridge operating modes from the FortiBridge CLI or by pressing the Mode button on the FortiBridge front panel. To switch operating modes from the CLI enter:

```
execute switch-mode
```

Backing up and restoring the FortiBridge configuration

Use the following procedures to backup and restore your FortiBridge configuration. For both of these procedures, you must have a TFTP server that you can connect to from any FortiBridge unit interface. The FortiBridge unit must be operating in normal mode.

To back up the FortiBridge configuration — Web-based manager

- 1 Go to *System > Status*.
- 2 In the System Configuration section, select the *Configuration Backup* link.
- 3 Your browser prompts you for the file name and location of the configuration file.

Using the web-based manager, the configuration backup file is saved to the computer you are using.

To back up the FortiBridge configuration — CLI

- 1 Make sure that the TFTP server is running.
- 2 Log into the FortiBridge CLI.
- 3 Backup the system configuration to a text file on the TFTP server. Enter:

```
execute backup config <filename_str> <tftp-server_ipv4>
```

The config file is copied to the TFTP server and saved with the specified file name.

To restore the FortiBridge configuration — Web-based manager

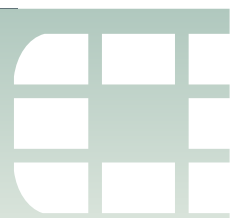
- 1 Go to *System > Status*.
- 2 In the System Configuration section, select the *Configuration Restore* link.
- 3 Select *Browse* and find the configuration backup file you want to restore.
- 4 Select *OK* to begin the restore procedure.
- 5 The FortiBridge unit reboots after loading the configuration file. While the FortiBridge unit is rebooting, all network traffic passes directly from INT1 and EXT1 bypassing the FortiGate unit.

To restore the FortiBridge configuration — CLI

- 1 Make sure that the TFTP server is running.
- 2 Log into the FortiBridge CLI.
- 3 Restore the system configuration from a text file on the TFTP server. Enter:

```
execute restore config <filename_str> <tftp-server_ipv4>
```

The config file is copied from the TFTP server to the FortiBridge unit. The FortiBridge unit reboots after loading the new configuration. While the FortiBridge unit is rebooting, all network traffic passes directly from INT1 and EXT1 bypassing the FortiGate unit.



Appendix

Document conventions

Fortinet technical documentation uses the conventions described below.

IPv4 IP addresses

To avoid publication of public IPv4 IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at <http://ietf.org/rfc/rfc1918.txt?number-1918>.

Most of the examples in this document use the following IP addressing:

IP addresses are made up of A.B.C.D:

- A - can be one of 192, 172, or 10 - the private addresses covered in RFC 1918.
- B - 168, or the branch / device / virtual device number.
 - Branch number can be 0xx, 1xx, 2xx - 0 is Head office, 1 is remote, 2 is other.
 - Device or virtual device - allows multiple FortiGate units in this address space (VDMs).
 - Devices can be from x01 to x99.
- C - interface - FortiGate units can have up to 40 interfaces, potentially more than one on the same subnet
 - 001 - 099- physical address ports, and non -virtual interfaces
 - 100-255 - VLANs, tunnels, aggregate links, redundant links, vdom-links, etc.
- D - usage based addresses, this part is determined by what the device is doing. The following gives 16 reserved, 140 users, and 100 servers in the subnet.
 - 001 - 009 - reserved for networking hardware, like routers, gateways, etc.
 - 010 - 099 - DHCP range - users
 - 100 - 109 - FortiGate devices - typically only use 100
 - 110 - 199 - servers in general (see later for details)
 - 200 - 249 - static range - users
 - 250 - 255 - reserved (255 is broadcast, 000 not used)
 - The D segment servers can be farther broken down into:
 - 110 - 119 - Email servers
 - 120 - 129 - Web servers
 - 130 - 139 - Syslog servers
 - 140 - 149 - Authentication (RADIUS, LDAP, TACACS+, FSAE, etc)
 - 150 - 159 - VoIP / SIP servers / managers
 - 160 - 169 - FortiAnalyzers
 - 170 - 179 - FortiManagers
 - 180 - 189 - Other Fortinet products (FortiScan, FortiDB, etc.)
 - 190 - 199 - Other non-Fortinet servers (NAS, SQL, DNS, DDNS, etc.)
 - Fortinet products, non-FortiGate, are found from 160 - 189.

Example Network

Variations on network shown in [Figure 40](#) are used for many of the examples in this document. In this example, the 172.20.120.0 network is equivalent to the Internet. The network consists of a head office and two branch offices.

Figure 40: Example network

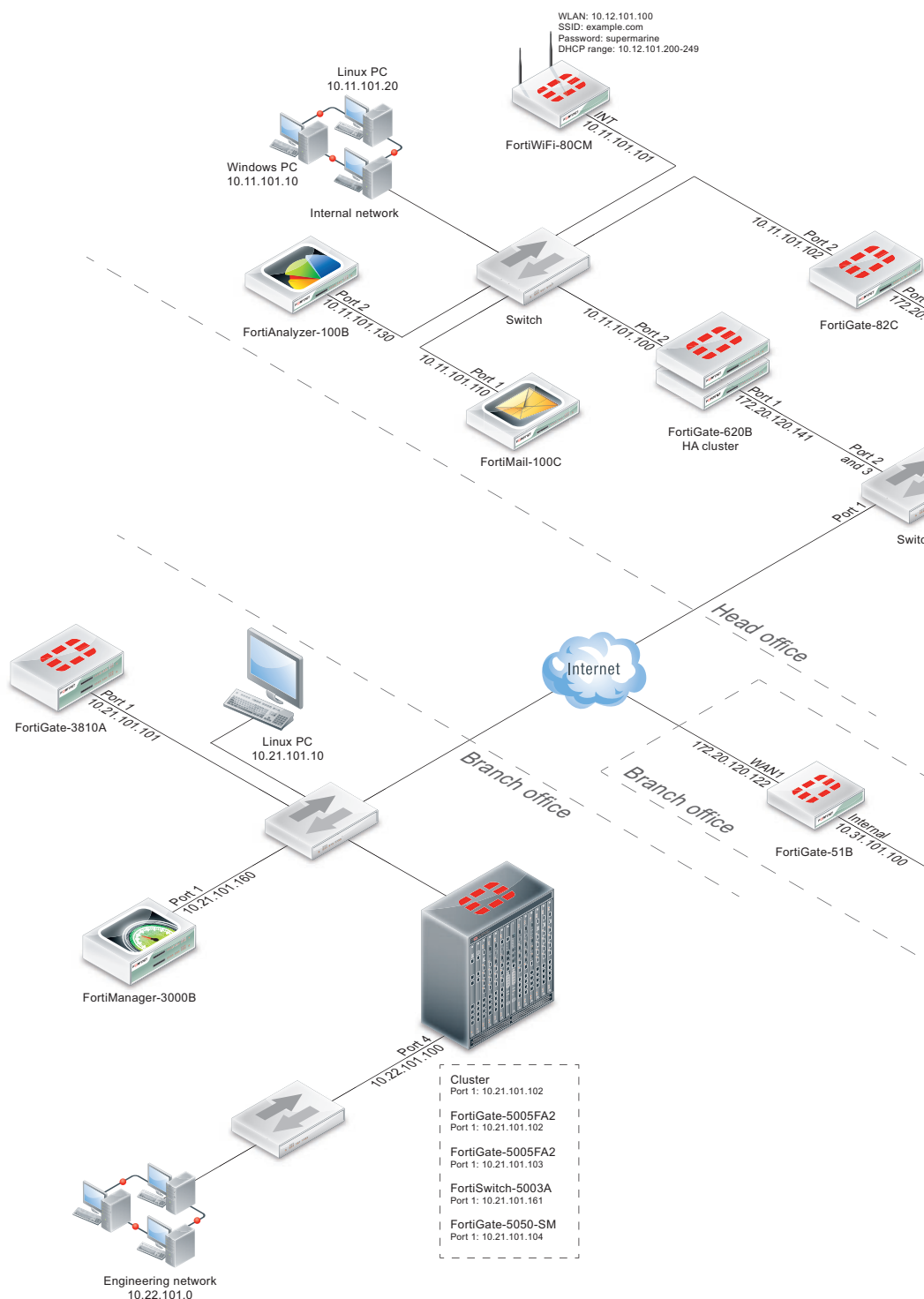


Table 8: Example IPv4 IP addresses

Location and device	Internal	Dmz	External
Head Office, one FortiGate	10.11.101.100	10.11.201.100	172.20.120.191
Head Office, second FortiGate	10.12.101.100	10.12.201.100	172.20.120.192
Branch Office, one FortiGate	10.21.101.100	10.21.201.100	172.20.120.193
Office 7, one FortiGate with 9 VDOMs	10.79.101.100	10.79.101.100	172.20.120.194
Office 3, one FortiGate, web server	n/a	10.31.201.110	n/a
Bob in accounting on the corporate user network (DHCP) at Head Office, one FortiGate	10.0.11.101.200	n/a	n/a
Router outside the FortiGate	n/a	n/a	172.20.120.195

Tips, must reads, and troubleshooting



A Tip provides shortcuts, alternative approaches, or background information about the task at hand. Ignoring a tip should have no negative consequences, but you might miss out on a trick that makes your life easier.



A Must Read item details things that should not be missed such as reminders to back up your configuration, configuration items that must be set, or information about safe handling of hardware. Ignoring a must read item may cause physical injury, component damage, data loss, irritation or frustration.



A Troubleshooting tip provides information to help you track down why your configuration is not working.

Typographical conventions

Table 9: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>

Table 9: Typographical conventions in Fortinet technical documentation

Emphasis	HTTP connections are <i>not</i> secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD><BODY><H4>You must authenticate to use this service.</H4>
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com .
Keyboard entry	Type a name for the remote VPN peer or client, such as Central_Office_1.
Navigation	Go to VPN > IPSEC > Auto Key (IKE).
Publication	For details, see the <i>FortiOS Handbook</i> .

Registering your Fortinet product

Access to Fortinet customer services, such as firmware updates, support, and FortiGuard services, requires product registration. You can register your Fortinet product at <http://support.fortinet.com>.

Training Services

Fortinet Training Services offers courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet training programs serve the needs of Fortinet customers and partners world-wide.

Visit Fortinet Training Services at <http://campus.training.fortinet.com>, or email training@fortinet.com.

Technical Documentation

Visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>, for the most up-to-date technical documentation.

The Fortinet Knowledge Base provides troubleshooting, how-to articles, examples, FAQs, technical notes, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

Comments on Fortinet technical documentation

Send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

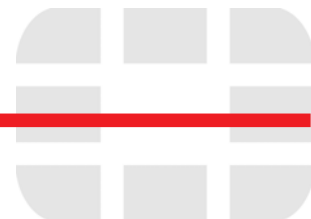
Customer service and support

Fortinet is committed to your complete satisfaction. Through our regional Technical Assistance Centers and partners worldwide, Fortinet provides remedial support during the operation phase of your Fortinet product's development life cycle. Our Certified Support Partners provide first level technical assistance to Fortinet customers, while the regional TACs solve complex technical issues that our partners are unable to resolve.

Visit Customer Service and Support at <http://support.fortinet.com>.

Fortinet products End User License Agreement

See the [Fortinet products End User License Agreement](#).



Index

Numerics

3DES, 41

A

action on failure, FortiBridge

- fail open, 81
- probe, 81
- send alertmail, 81
- SNMP trap, 81
- syslog, 81

active-active HA, 31, 37

administrator

- adding a FortiBridge password, 71

administrator accounts, FortiBridge

- adding, 73

ADM-XD4

- security processing module, 29

AES-128, 41

AES-192, 41

AES-256, 41

aggregation, link, 30, 31

alert email

- configuring the FortiBridge, 85
- sample FortiBridge message, 85

alertmail, FortiBridge

- action on failure, 81

alerts

- configuring the FortiBridge, 84

AMC

- bridge module, 20
- configuring AMC modules, 19

AMC (Advanced Mezzanine Card), 23

AMC module

- configuring, 19

anomaly

- checks, 46
- hardware checks, 46
- IPS checks, 46

antireplay, 41, 42, 43, 44, 45, 48, 49, 50, 51

antivirus, 31

application layer, 30

ASM-CX4, 20

ASM-cx4, 20

ASM-FX2, 20

B

backing up

- FortiBridge configuration, 88

bandwidth

- calculation method, 39
- limitation, 39

bandwidth guarantees, 31

basic FortiBridge configuration, 71

basic FortiBridge settings, 80

bidirection, 39

bridge mode, 20

bridge module

- AMC, 20

bypass mode, FortiBridge, 65

- connecting to a FortiBridge CLI, 66
- resuming normal mode, 88
- switching to normal mode, 66

C

certification, 94

CLI, 48

- connecting to a FortiBridge unit in bypass mode, 66
- resetting a FortiBridge unit to factory defaults, 74

cluster

- FortiBridge application, 67

cluster member, 38

community

- adding to a FortiBridge unit, 87
- SNMP on a FortiBridge unit, 87

configuration

- backing up and restoring a FortiBridge unit, 88
- basic FortiBridge configuration, 71

configuration example, FortiBridge

- HA cluster, 67
- other FortiGate interfaces, 68
- standalone FortiGate unit, 59

connect

- FortiBridge unit, 60

conventions, 91

cryptographic load, 40

customer service, 94

cx4, 20

D

date

- changing the FortiBridge system date, 73

decryption, 42, 43, 44, 45, 48, 49, 50, 51

default

- probe settings on a FortiBridge unit, 81
- resetting a FortiBridge unit to factory defaults, 74

DES, 41

DNAT, 30

DNS server

- changing DNS IP addresses on a FortiBridge unit, 72

documentation

- conventions, 91
- Fortinet, 94

dynamic IP pattern

- FortiBridge probe setting, 81

E

EEI (Enhanced Extension Interface), 26
 email
 alert, FortiBridge, 85
 encryption, 42, 43, 44, 45, 48, 49, 50, 51
 ESP, 41
 example configuration, FortiBridge, 59
 HA cluster, 67
 other FortiGate interfaces, 68
 example IPSec configurations, 42, 48
 execute shutdown, 17
 EXT1
 FortiBridge management access, 73

F

FA2 (NP1) processor, 25
 factory default
 resetting a FortiBridge unit, 74
 fail open, FortiBridge, 81
 recovering from, 87
 failure threshold
 tuning a FortiBridge unit, 84
 failure, FortiBridge
 recovering from, 87
 fast path
 required session characteristics, 30
 fast path requirements, 30
 firewall policy
 and FortiBridge probes, 63
 firmware
 install on a FortiBridge unit from a system reboot, 75
 installing on a FortiBridge unit, 74
 upgrading a FortiBridge unit to a new version, 74
 firmware install, 26
 FortiAccel (NP1) processor, 25
 FortiAnalyzer traffic reports, 24
 FortiBridge-2002
 connecting, 61
 FortiBridge-2002F
 connecting, 61
 FortiGate HA cluster
 FortiBridge application, 67
 FortiGate-ASM-CX4, 20
 FortiGate-ASM-FB4, 42, 48
 FortiGate-ASM-FX2, 20
 FortiGuard
 Antivirus, 94
 Fortinet
 Technical Documentation, conventions, 91
 Technical Support, 94
 Technical Support, registering with, 94
 Training Services, 94
 Fortinet customer service, 94
 Fortinet documentation, 94
 fragmented packets, 31
 frame size, 25
 frame size, maximum, 26
 front panel
 resetting FortiBridge unit to factory defaults, 74

FTP, 31
 configuring FortiBridge probe, 83
 FortiBridge probe, 64
 FX2, 20

G

grounding, 10

H

HA cluster
 FortiBridge application, 67
 HA session offloading, 37
 high availability (HA), 37
 active-active, 31
 load balancing, 31
 HMAC check offloading, 41
 HTTP
 FortiBridge probe, 64

I

ICMP land, 47
 IEEE 802.1q, 30
 IEEE 802.3ad, 30
 IMAP
 FortiBridge probe, 64
 installing
 FortiBridge unit firmware, 74
 interface mode, 44, 50
 interface mode IPSec, 48
 interval
 FortiBridge probe, 65
 introduction
 Fortinet documentation, 94
 Intrusion Prevention, 46
 Intrusion Prevention System (IPS), 31, 46
 IP address
 private network, 91
 IP land, 47
 IPSec, 23, 25, 31, 41, 42, 43, 44, 48, 49, 50
 interface mode, 48
 tunnel, 40
 tunnel mode, 48
 IPSec Interface Mode, 45, 48, 50, 51
 IPv4, 30
 ISAKMP, 41

J

jumbo frames, 26

L

Layer 2, 30
 Layer 3, 30
 Layer 4, 30
 layer-2 bridge, FortiBridge, 60
 link aggregation, 30, 31
 load balancing, 31, 37
 Local Gateway IP, 40, 43, 44, 45, 48, 49, 50, 51
 local host, 31, 40, 42

- log message, FortiBridge, 81
 - sample, 86

- logging
 - configuring a FortiBridge unit, 86
 - syslog, FortiBridge, 85

- loose source record route, 47

M

- Main Interface IP, 48

- management access to the FortiBridge EXT1 interface, 73

- management IP
 - changing the FortiBridge management IP address, 71
 - FortiBridge, 60

- master unit, 38

- maximum frame size, 26

- MD5, 41

- mode
 - switching between FortiBridge modes, 66

- monitor
 - how a FortiBridge unit monitors a FortiGate unit, 62

- MTU (Maximum Transmission Unit), 26, 31

N

- network
 - topology, 42, 48

- network processing unit (NPU), 38, 41

- network processors
 - FA2 (NP1), 25
 - FortiAccel (NP1), 25
 - NP1, 25
 - NP2, 25
 - NP4, 25

- normal mode, FortiBridge, 60, 62
 - monitoring the FortiGate unit, 62
 - probe, 62
 - resuming from bypass mode, 88
 - switching to, 66
 - switching to bypass mode, 66
 - traffic flow, 62

- NP1, 26, 31, 41

- NP1 processor, 25

- NP2, 26

- NP2 processor, 25

- NP4 processor, 25

O

- operating modes, FortiBridge
 - switching between, 88

- operating principles, 59

P

- P2 Proposal, 48

- packet
 - forwarding rate, 24, 25, 42, 48
 - processing flow, 23

- packet flow, 23

- password
 - adding to a FortiBridge, 71

- Phase 1, 41, 43, 44, 45, 48, 49, 50, 51

- Phase 2, 42, 43, 44, 45, 48, 49, 50, 51

- Phase I, 40

- Phase II, 41

- ping
 - enabling FortiBridge ping probes, 83
 - FortiBridge probe, 63

- policy, 31

- POP3
 - probe, FortiBridge, 64

- power failure
 - FortiBridge, 66

- power off, 17

- primary unit, 38

- probe interval
 - tuning a FortiBridge unit, 84

- probe list
 - FTP, 83
 - ping, 83
 - SMTP, 83

- probe, FortiBridge, 62
 - action on failure, 81
 - and FortiGate firewall policies, 63
 - configuring, 80
 - configuring FortiGate unit, 82
 - configuring probe settings, 81
 - default FortiBridge settings, 81
 - enabling, 82
 - enabling FortiBridge ping probes, 83
 - enabling probes, 82, 83
 - fail open, 81
 - FortiBridge dynamic IP pattern, 81
 - FortiGate hardware failure, 65
 - FortiGate session list, 84
 - FortiGate software failure, 65
 - FortiGate unit serial number, 81
 - FTP, 64
 - HTTP, 64
 - IMAP, 64, 83
 - interval, 65
 - ping, 63
 - POP3, 64
 - settings, 81
 - SMTP, 64, 83
 - threshold, 65
 - verifying, 84
 - viewing probe configuration, 83

- product registration, 94

Q

- QoS, 31, 39

R

- RAID, 53
 - configuring, 54
 - levels, 53
 - rebuilding an array, 56

- rate limits, 31

- reboot
 - installing FortiBridge firmware, 75
- record route option, 47

- recover
 - from a FortiGate failure, 87
- registering
 - with Fortinet Technical Support, 94
- replay detection, 41, 42, 43, 45, 48, 49, 50, 51
- reset
 - factory default FortiBridge configuration, 74
- restoring
 - FortiBridge configuration, 88
- RFC
 - 1918, 91
- route, 44, 45, 46, 49, 50, 51
 - adding static routes to a FortiBridge unit, 72

S

- security association (SA), 23, 41, 42
- security option, 47
- security processing modules, 28
 - displaying information, 29
 - models, 29
- send alertmail from FortiBridge unit, 81
- session
 - key, 23
- session helper, 31
- session list
 - showing FortiBridge probes, 84
- settings
 - configuring FortiBridge probe settings, 81
- SHA1, 41
- shut down, 17
- slave unit, 38
- SMTP
 - FortiBridge probe list, 83
 - probe, FortiBridge, 64
- SNAT, 30
- SNMP
 - adding a community to a FortiBridge unit, 87
 - configuring on a FortiBridge unit, 86
 - FortiBridge unit community, 87
 - trap, FortiBridge, 81
- static route, 44, 45, 46, 49, 50, 51
 - adding static routes to a FortiBridge unit, 72
- stream option, 47
- strict source record route, 47
- switch
 - switching between FortiBridge modes, 66
- switching
 - between FortiBridge operating modes, 88
- syslog
 - configuring a FortiBridge unit, 86
 - sample FortiBridge message, 86

- syslog message, 81

T

- TCP land, 47
- TCP WinNuke, 47
- technical
 - documentation conventions, 91
 - support, 94
- technical support, 94
- TFTP, 26
- threshold, FortiBridge
 - probe, 65
- time
 - changing the FortiBridge system time, 73
- timestamp option, 47
- topology, 42, 48
- traffic flow
 - normal FortiBridge mode, 62
- traffic offloading, 30
- traffic shaping, 31, 39
- traffic shaping offloading, 38
- traffic statistics, 24
- Training Services, 94
- transparent mode
 - example FortiBridge network, 60
- TTL reduction, 30
- tunnel mode, 43, 49
- tunnel mode IPSec, 48

U

- UDP land, 47
- unidirection, 39
- unknown option, 47
- unknown protocol, 47
- upgrading
 - FortiBridge firmware, 74

V

- verifying
 - FortiBridge probes, 84
- VLAN, 30
- VPN, 41
 - gateway, 44, 49, 50
- VPN encryption/decryption offloading, 41

W

- wire speed, 25