FortiGate-6000 - Handbook

Version 6.0.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 6, 2019
FortiGate-6000 6.0.4 Handbook
01-604-465651-20191206

TABLE OF CONTENTS

Change log

Date	Change description
December 6, 2019	Corrections to FortiGate-6000 IPsec VPN on page 42 and FortiGate-6000 IPsec VPN load balancing on page 42. New sections: ICAP support on page 62 and SSL mirroring support on page 64.
July 10, 2019	Changes to Managing individual management boards and FPCs in HA mode on page 51. New section: Adding a flow rule to support DHCP relay on page 33. Additional changes and fixes throughout the document.
June 21, 2019	New section: Default Security Fabric configuration on page 66.
April 30, 2019	Fixes and updates throughout the document.
April 26, 2019	Fixes and updates throughout the document.
April 26, 2019	FortiOS 6.0.4 document release.

What's new for FortiGate-6000 6.0.4

The following new features have been added to FortiGate-6000 and FortiGate-7000 v6.0.4 build 6145:

- Diagnose debug flow trace output improvements, see Diagnose debug flow trace for FPC and management board activity on page 26.
- New diagnose command to show how the DP3 processor will load balance a session, see Showing how the DP3 processor will load balance a session on page 27.
- Enabling or disabling synchronizing connectionless sessions, see Enabling session pickup for TCP SCTP and connectionless sessions on page 57.
- ICMP traffic can now be load balanced, see ICMP load balancing on page 1.
- FortiGate Session Life Support Protocol (FGSP) support, see FortiGate-6000 FGSP HA on page 58.

FortiGate-6000 overview

The FortiGate-6000 series is a collection of 3U 19-inch rackmount appliances that all include twenty-four 25GigE SFP28 and four 100GigE QSFP28 data network interfaces, as well as NP6 and CP9 processors to deliver high IPS/threat prevention performance.

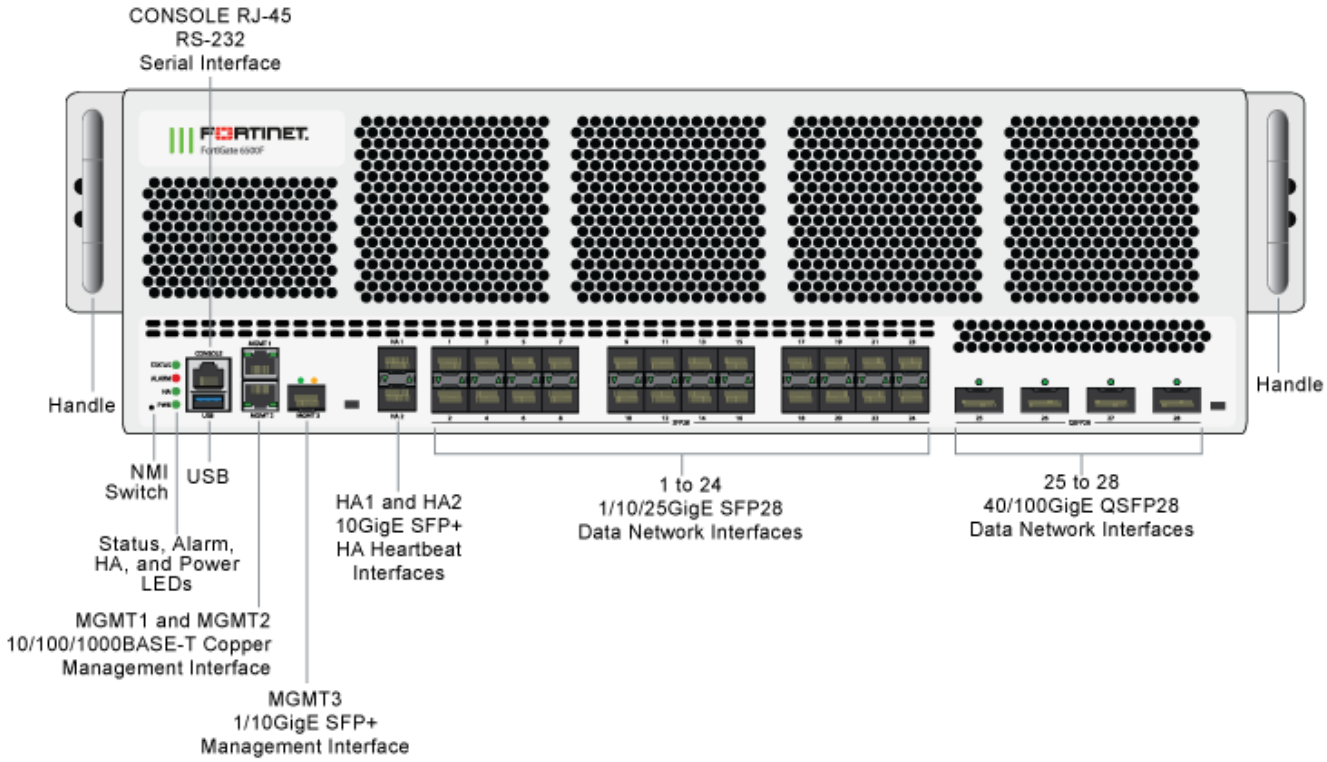
Currently, four FortiGate-6000 models are available:

- FortiGate-6500F
- FortiGate-6501F
- FortiGate-6300F
- FortiGate-6301F

All FortiGate-6000 models have the same front and back panel configuration including the same network interfaces. The differences are the processing capacity of the individual models. All FortiGate-6000 models include internal Fortinet Processor Cards (FPCs) that contain NP6 and CP9 security processors. The FortiGate-6000 uses session-aware load balancing to distribute sessions to the FPCs. The FortiGate-6500F includes ten FPCs and the FortiGate-6300F includes six FPCs.

Also the FortiGate-6501F and 6301F models are the same as their related models with the addition of two internal 1 TByte log disks.

FortiGate-6000 front panel (FortiGate-6500F shown)



Front panel interfaces

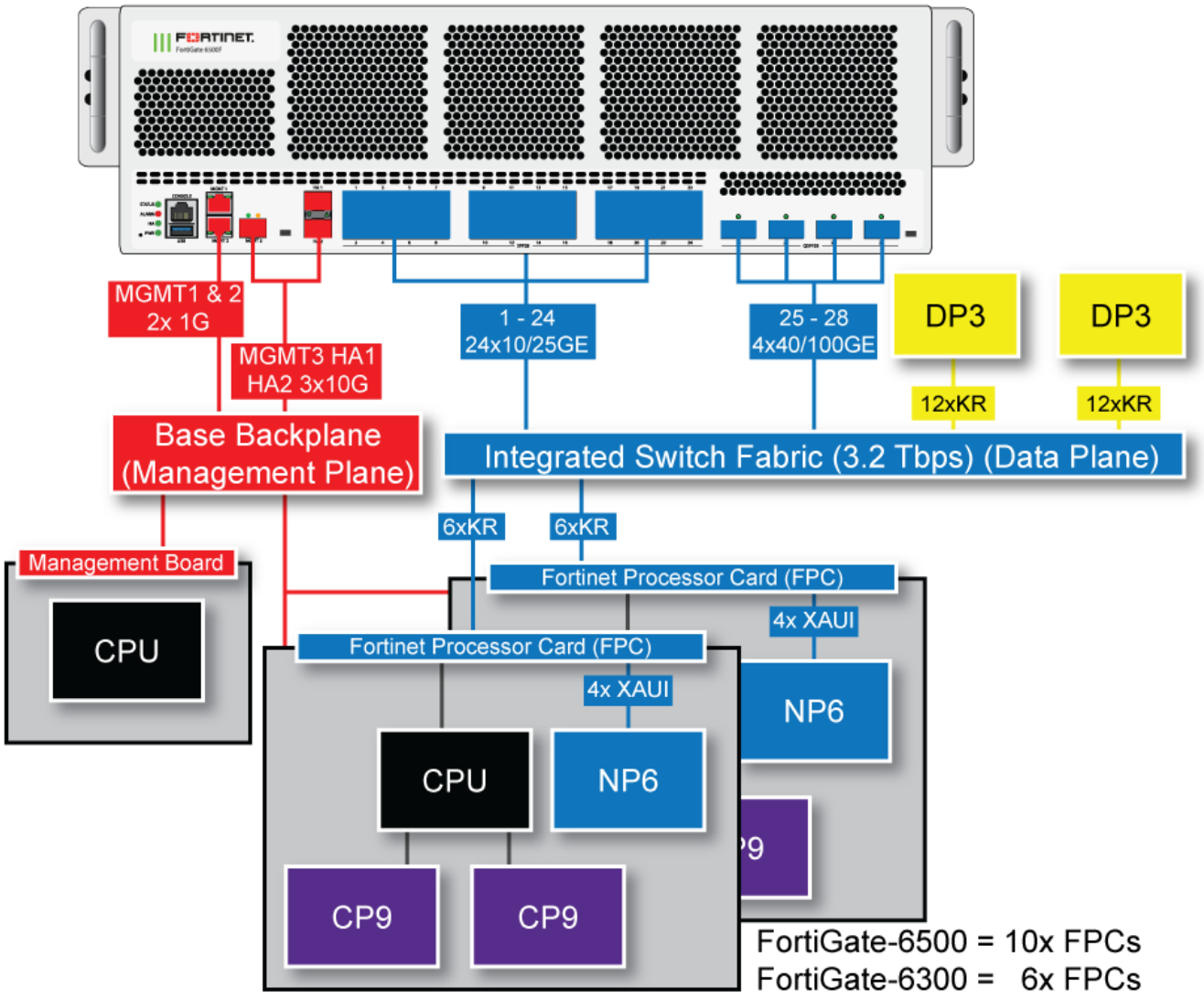
All FortiGate-6000 models have the following front panel interfaces:

- Twenty-four 1/10/25GigE SFP28 data network interfaces (1 to 24). The default speed of these interfaces is 10Gbps.
- Four 40/100GigE QSFP28 data network interfaces (25 to 28). The default speed of these interfaces is 40Gbps.
- Two front panel 1/10GigE SFP+ HA interfaces (HA1 and HA2) used for heartbeat, session sync, and management communication between two and only two FortiGate-6000s in an HA cluster. The default speed of these interfaces is 10Gbps. Operating them at 1Gbps is not recommended. A FortiGate-6000 cluster consists of two (and only two) FortiGate-6000s of the same model. To set up HA, you can use a direct cable connection between the FortiGate-6000s HA1 interfaces and a second direct cable connection between the HA2 interfaces. For more information about FortiGate-6000 HA, see FortiGate-6000 high availability on page 44.
- Two 10/100/1000BASE-T out of band management Ethernet interfaces (MGMT1 and MGMT2).
- One front panel 1/10GigE SFP+ out of band management interface (MGMT3). You can use the 10Gbps MGMT3 interface for additional bandwidth management traffic that might be useful for high bandwidth activities such as remote logging.
- One RJ-45 RS-232 serial console connection.
- One USB connector.

FortiGate-6000 schematic

The FortiGate-6000 has separate data and management planes. The data plane handles all traffic and security processing functionality. The management plane handles management functions such as administrator logins, configuration and session synchronization, SNMP and other monitoring, HA heartbeat communication, and remote and (if supported) local disk logging. Separating these two planes means that resources used for traffic and security processing are not compromised by management activities.

FortiGate-6000 schematic



In the data plane, two DP3 load balancers use session-aware load balancing to distribute sessions from the front panel interfaces (port1 to 28) to Fortinet Processor Cards (FPCs). The DP3 processors communicate with the FPCs across the 3.2Tbps integrated switch fabric. Each FPC processes sessions load balanced to it. The FPCs send outgoing sessions back to the integrated switch fabric and then out the network interfaces to their destinations.

The NP6 processor in each FPC enhances network performance with fastpath acceleration that offloads communication sessions from the FPC CPU. The NP6 processor can also handle some CPU intensive tasks, like IPsec VPN encryption/decryption.

The CP9 processors in each FPC accelerate many common resource intensive security related processes such as SSL VPN, Antivirus, Application Control, and IPS.

The management plane includes the management board, base backplane, management interfaces, and HA heartbeat interfaces. Configuration and session synchronization between FPCs in a FortiGate-6000F occurs over the base backplane. In an HA configuration, configuration and session synchronization between the FortiGate-6000s in the

cluster takes place over the HA1 and HA2 interfaces. Administrator logins, SNMP monitoring, remote logging to one or more FortiAnalyzers or syslog servers, and other management functions use the MGMT1, MGMT2, and MGMT3 interfaces. You can use the 10Gbps MGMT3 interface for additional bandwidth that might be useful for high bandwidth activities such as remote logging.

Interface groups and changing data interface speeds

Depending on the networks that you want to connect your FortiGate-6000 to, you may have to manually change the data interface speeds. The port1 to port24 data interfaces are divided into the following groups:

- port1 - port4
- port5 - port8
- port9 - port12
- port13 - port16
- port17 - port20
- port21 - port24

All of the interfaces in a group operate at the same speed. Changing the speed of an interface changes the speeds of all of the interfaces in the same group. For example, if you change the speed of port18 from 10Gbps to 25Gbps the speeds of port17 to port20 are also changed to 25Gbps.

Another example, the default speed of the port1 to port24 interfaces is 10Gbps. If you want to install 25GigE transceivers in port1 to port24 to convert these data interfaces to connect to 25Gbps networks, you must enter the following from the CLI:

```
config system interface
   edit port1
      set speed 25000full
   next
   edit port5
      set speed 25000full
   next
   edit port9
      set speed 25000full
   next
   edit port13
      set speed 25000full
   next
   edit port17
      set speed 25000full
   next
   edit port21
      set speed 25000full
   end
```

Every time you change a data interface speed, when you enter the `end` command, the CLI confirms the range of interfaces affected by the change. For example, if you change the speed of port5 the following message appears:

```
config system interface
   edit port5
   set speed 25000full
end
port5-port8 speed will be changed to 25000full due to hardware limit.
Do you want to continue? (y/n)
```

Getting started with FortiGate-6000

After you install your FortiGate-6000 in a rack and connect it to power, you should review the front and back panel LEDs to verify that everything is operating normally.

Normal operation: front and back panel LEDs

When your FortiGate-6000 is operating normally, the front panel LEDs should appear as follows.

LED	State
Status	Green
Alarm	Off
HA	Off
Power	Green
Connected network interfaces	Solid or flashing green.

During normal operation, the back panel PSU and fan try LEDs should all be solid green. This indicates that each component has power and is operating normally.

When the system has initialized, you have a few options for connecting to the FortiGate-6000 GUI or CLI:

- Log in to the management board GUI by connecting MGMT1 or MGMT2 to your network and browsing to https://192.168.1.99 or https://192.168.2.99.
- Log in to the management board CLI by connecting MGMT1 or MGMT2 to your network and using an SSH client to connect to 192.168.1.99 or 182.168.2.99.
- Log in to the management board CLI by connecting to the RJ-45 RS-232 CONSOLE port with settings: BPS: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.

The FortiGate-6000 ships with the following factory default configuration.

Option	Default Configuration
Administrator Account User Name	admin
Password	(none) For security reasons you should add a password to the admin account before connecting the FortiGate-6000 to your network.
MGMT1 IP/Netmask	192.168.1.99/24
MGMT2 IP/Netmask	192.168.2.99/24

All configuration changes must be made from the management board GUI or CLI and not from individual FPCs.

All other management communication (for example, SNMP queries, remote logging, and so on) use the MGMT1 or MGMT2 interfaces and are handled by the management board.

Default VDOM configuration and configuring the management interfaces

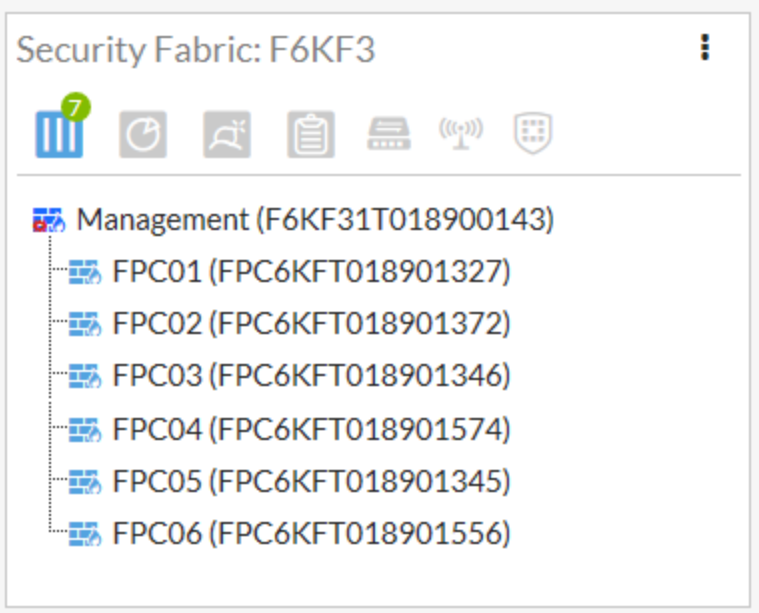
The default FortiGate-6000 configuration includes a management VDOM named **mgmt-vdom**. The mgmt1, mgmt2, mgmt3, ha1, and ha2 interfaces are in this VDOM. You cannot delete or rename this VDOM. You also cannot remove interfaces from it or add interfaces to it. You can however, configure other settings such as routing for management communications, mgmt1 and mgmt2 interface IP addresses, and so on.

Confirming startup status

Before verifying normal operation and making configuration changes and so on you should wait until the FortiGate-6000 is completely started up and synchronized. This can take a few minutes.

To confirm that the FortiGate-6000 is synchronized, view the **Security Fabric** dashboard widget. If the system is synchronized, the management board and all of the FPCs should be visible and ForGate telemetry status should be **Connected**. The widget also indicates if any FPCs are not synchronized. You can also view the **Sensor Information** widget to confirm that the system temperatures are normal and that all power supplies and fans are operating normally.

Example FortiGate-6301F Security Fabric widget showing normal operation



From the CLI you can use the `diagnose sys confsync status | grep in_sy` command to view the synchronization status of the management board and FPCs. If all of the FPCs are synchronized, each output line should include `in_sync=1`. If a line ends with `in_sync=0`, that FPC is not synchronized. The following example just shows a few output lines:

```
diagnose sys confsync status | grep in_sy
FPC6KF3E17900200, Slave, uptime=5385.45, priority=119, slot_id=2:1, idx=2, flag=0x4, in_sync=1
F6KF313E17900031, Slave, uptime=5484.74, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
F6KF313E17900032, Master, uptime=5488.57, priority=1, slot_id=2:0, idx=1, flag=0x10, in_sync=1
```

```
FPC6KF3E17900201, Slave, uptime=5388.78, priority=120, slot_id=2:2, idx=2, flag=0x4, in_sync=1
F6KF313E17900031, Slave, uptime=5484.74, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
...
```

Configuration synchronization

Wen you log into the FortiGate-6000 GUI or CLI by connecting to the IP address of the MGMT1 or MGMT2 interface, or through a console connection, you are logging into the FortiGate-6000 management board (part of the FortiGate-6000 management plane). The management board is the FortiGate-6000 config-sync master. All configuration changes must be made from the management board GUI or CLI. The management board synchronizes configuration changes to the FPCs and makes sure FPC configurations remain synchronized with the management board.

Once you have logged into the management board GUI or CLI and verified that the system is operating normally, you can view and change the configuration of your FortiGate-6000 just like any FortiGate. For example, you can configure firewall policies between any two interfaces. You can also configure aggregates of the front panel interfaces.

FortiGate-6000 dashboard widgets

The FortiGate-6000 includes a number of custom dashboard widgets that provide extra or custom information for FortiGate-6000 systems.

Security Fabric

The **Security Fabric** widget shows the components in your FortiGate-6000 system including the management board and FPCs. You can hover over the components in the Security Fabric widget to see each component's host name, serial number, model, firmware version, and management IP address. The Security Fabric widget also indicates if the FPCs are synchronized and communicating with the management board and identifies the primary (master) FPC.

Interface Bandwidth

You can create multiple **Interface Bandwidth** widgets to show traffic that is transmitted and received by any FortiGate-6000 interface. You can create **Interface Bandwidth** widgets for:

- Any physical interface
- Any link aggregation (LAG) interface
- Any redundant interface
- Any individual member of a LAG or a redundant interface
- Any VLAN interface
- Any IPsec VPN tunnel interface

Interface bandwidth widgets display all of the traffic processed by the interface, independently of how the traffic is load balanced.

You can create individual **Interface Bandwidth** widgets for each interface that you want to monitor. After you create a widget, you can choose to display traffic for the last hour, 24 hours, or week, updated in real time.

To display similar information from the CLI for physical interfaces, use the following command:

```
diagnose hardware deviceinfo nic <interface-name>
```

To display similar information from the CLI for LAG and VLAN interfaces, use the following command:

```
diagnose netlink interface list <interface-name>
```

Resource Usage

You can create multiple **Resource Usage** widgets to show CPU use, disk usage (on the FortiGate-6301F and 6501F), log rate, memory use, session creation rate, and the number of active sessions. You can create separate widgets for management traffic and for data traffic. After you have created a widget, you can choose to display data for the last 1 minute to 24 hours updated in real time.

Sensor Information

The Sensor Information dashboard widget displays FortiGate-6000 temperature, power supply (PSU), and fan speed information. You can click on any item on the widget to display data collected by individual sensors.

Using data interfaces for management traffic

The FortiGate-6000 supports basic management communication through the FortiGate-6000 data interfaces (port1 to port28). To enable management connections to these interfaces, configure the VDOM that the data interfaces are included in to allow traffic forwarding to the management board.

For example, to allow management communication for interfaces in the root VDOM, edit the root VDOM from the CLI and use the following command:

```
config vdom
   edit root
      config system settings
         set motherboard-traffic-forwarding icmp admin
      end
```

The `icmp` option, enabled by default, allows you to log into the management board from one of the MGMT interfaces and use the `execute ping` command to ping an address through one of the data interfaces. The interface used depends on the routing configuration.

The `admin` option allows Telnet, SSH, HTTP, and HTTPS management connections a data interface in the VDOM. You cannot configure data interfaces to accept management connections using non-standard ports.

You can enable both `icmp` and `admin` traffic forwarding or just one or the other.

Currently, the `admin` option is in development and not recommended.

Managing individual FPCs

In some cases, you may want to connect to the individual FPCs. For example, you may want to view traffic being processed by a specific FPC. You can connect to the GUI or CLI of individual FPCs using the MGMT1 interface IP address with a special port number.

For example, if the MGMT1 interface IP address is 192.168.1.99 you can connect to the GUI of the first FPC (the FPC in slot 1) by browsing to :

```
https://192.168.1.99:44301
```

The special port number (in this case, 44301) is a combination of the service port (for HTTPS, the service port is 443) and the FPC slot number (in this example, 01). The following table lists the special ports to use to connect to each FPC slot using common management protocols. The FortiGate-6300F and 6301F have 7 slots (0 to 6) and the FortiGate-6500F and 6501F have 11 slots (0 to 10). Slot 0 is the management board (MBD) slot. Slots 1 to 10 are FPC slots.

FortiGate-6000 special management port numbers

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8000	44300	2300	2200	16100
Slot 1 (FPC01)	8001	44301	2301	2201	16101
Slot 2 (FPC02)	8002	44302	2302	2202	16102
Slot 3 (FPC03)	8003	44303	2303	2203	16103
Slot 4 (FPC04)	8004	44304	2304	2204	16104
Slot 5 (FPC05)	8005	44305	2305	2205	16105
Slot 6 (FPC06)	8006	44306	2306	2206	16106
Slot 7 (FPC07)	8007	44307	2307	2207	16107
Slot 8 (FPC08)	8008	44308	2308	2208	16108
Slot 9 (FPC09)	8009	44309	2309	2209	16109
Slot 10 (FPC10)	8010	44310	2310	2210	16110

For example, to connect to the CLI of the FPC in slot 3 using SSH, you would connect to ssh://192.168.1.99:2203.

To verify which slot you have logged into, the GUI header banner and the CLI prompt shows its hostname. The CLI prompt also shows slot address in the format `<hostname> [<slot address>] #`.

Logging in to different FPCs allows you to use the FortiView or Monitor GUI pages to view the activity on that FPC. Even though you can log in to different FPCs, you can only make configuration changes from the management board.

Connecting to individual FPC consoles

From the management board CLI, you can use the `execute system console-server` command to access to individual FPC consoles. Console access can be useful for troubleshooting. For example, if an FPC does not boot

properly, you can use console access to view the state of the FPC and enter commands to fix the problem or restart the FPC.

From the console, you can also perform BIOS-related operations, such as rebooting the FPC, interrupting the boot process, and installing new firmware.

For example, from the management board CLI, use the following command to log in to the console of the FPC in slot 3:

```
execute system console-server connect 3
```

Authenticate to log in to the console and use CLI commands to view information, make changes, or restart the FPC. When you are done, use **Ctrl-X** to exit from the console back to the management board CLI. Using **Ctrl-X** may not work if you are accessing the CLI console from the GUI. Instead you may need to log out of the GUI and then log in again.

Also from the management board CLI you can use the `execute system console-server showline` command to list any active console server sessions. Only one console session can be active for each FPC, so before you connect to an FPC console, you can use the following command to verify whether or not there is an active console session. The following command output shows an active console session with the FPC in slot 4:

```
execute system console-server showline
MB console line connected - 1
Telnet-to-console line connected - 4
```

To clear an active console session, use the `execute system console-server clearline` command . For example, to clear an active console session with the FPC in slot 4, enter:

```
execute system console-server clearline 4
```

In an HA configuration, the `execute system console-server` commands only allow access to FPCs in the FortiGate-6000 that you are logged into. You can't use this command to access FPCs in the other FortiGate-6000 in an HA cluster

Connecting to individual FPC CLIs

From the management board CLI you can use the following command to switch between FPCs and perform different operations on the FPC in each slot:

```
execute load-balance slot {manage | nmi-reset | power-off | power-on | reboot} <chassis-
     number>.<slot-number>
```

Use `manage` to connect to the CLI of a different FPC. Use the other options to perform an action on an individual FPC.

For example, to connect to the FPC in chassis 1 slot 4, enter the following command:

```
execute load-balance slot manage 1.4
```

To reboot the FPC in chassis 1 slot 3, enter the following command:

```
execute load-balance slot reboot 1.3
```

From any CLI you can also use the `execute load-balance slot manage [<chassis>.]<slot>` command to log into the CLI of any FPC. You can use this command to view the status or configuration of the FPC, restart the FPC, or perform other operations. You should not change the configuration of individual FPCs because this can cause configuration synchronization errors.

`<chassis>` is the HA chassis ID and can be 1 or 2. The chassis ID is required only in an HA configuration where you are attempting to log in to the other chassis. In HA mode, if you skip the chassis ID, you can log in to another component in the same chassis.

<slot> is the slot number of the component that you want to log in to. The management board is in slot 0 and the FPC slot numbers start at 1.

For example, in a FortiGate-6000 standalone configuration, if you logged in to the CLI of the management board, enter the following command to log in to the FPC in slot 5:

```
execute load-balance slot manage 5
```

In a FortiGate-6000 HA configuration, if you logged into the CLI of the management board in chassis 1, enter the following command to log into the FPC in chassis 2 slot 5:

```
execute load-balance slot manage 2.5
```

In a FortiGate-6000 HA configuration, if you logged into the CLI of the management board in chassis 2, enter the following command to log in to the FPC in chassis 1 slot 3:

```
execute load-balance slot manage 1.3
```

In a FortiGate-6000 HA configuration, if you logged in to the CLI of the management board in chassis 1, enter the following command to log in to the FPC in slot 3 of the same chassis:

```
execute load-balance slot manage 3
```

After you log in to a different component in this way, you can't use the `execute load-balance slot manage` command to log into another component. Instead you must use the `exit` command to revert back to the CLI of the component that you originally logged into. Then, you can use the `execute load-balance slot manage` command to log in to another component.

Connecting to FPC CLIs using the console port

If you connect a PC to the FortiGate-6000 console port with a serial cable and open a terminal session, you are connected to the management board CLI. You can press Ctrl-T to enable console switching mode. Pressing Ctrl-T multiple times cycles through the management board (MBD) CLI and FPC CLIs. Once you have connected to the CLI that you want to use, press Enter to enable the CLI and login.

Firmware upgrades

The management board and the FPCs in your FortiGate-6000 system run the same firmware image. You upgrade the firmware using the management board GUI or CLI just as you would any FortiGate product. During the upgrade process, the firmware running on the management board and all of the FPCs upgrades in one step. Firmware upgrades should be done during a quiet time because traffic will be briefly interrupted during the upgrade process. The entire firmware upgrade takes a few minutes, depending on the number of FPCs in your FortiGate-6000 system. Some firmware upgrades may take longer depending on factors, such as the size of the configuration and whether an upgrade of the DP processor is included.

Before beginning a firmware upgrade, Fortinet recommends that you perform the following tasks:

- Review the latest release notes for the firmware version that you are upgrading to.
- Verify the recommended upgrade path, as documented in the release notes.
- Back up your FortiGate-6000 configuration.

Fortinet recommends that you review the services provided by your FortiGate-6000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

If you are operating two FortiGate-6000s in HA mode with `uninterruptable-upgrade` and `session-pickup` enabled, firmware upgrades should only cause a minimal traffic interruption. Use the following command to enable these settings. These settings are synchronized to all FPCs.

```
config system ha
   set uninterruptable-upgrade enable
   set session-pickup enable
end
```

Installing firmware on an individual FPC

You may want to install firmware on an individual FPC to resolve a software-related problem with the FPC or if the FPC is not running the same firmware version as the management board. The following procedure describes how to transfer a new firmware image file to the FortiGate-6000 internal TFTP server and then install the firmware on an FPC.

1. Copy the firmware image file to a TFTP server, FTP server, or USB key.
2. To upload the firmware image file onto the FortiGate-6000 internal TFTP server, from the management board CLI, enter one of the following commands.
   - To upload the firmware image file from an FTP server:
     ```
     execute upload image ftp <image-file-and-path> <comment> <ftp-server-address>
          <username> <password>
     ```
   - To upload the firmware image file from a TFTP server:
     ```
     execute upload image tftp <image-file> <comment> <tftp-server-address>
     ```
   - To upload the firmware image file from a USB key:
     ```
     execute upload image usb <image-file-and-path> <comment>
     ```
3. Enter the following command to install the firmware image file on to an FPC:
   ```
   execute load-balance update image <slot-number>
   ```
   where `<slot-number>` is the FPC slot number.

   This command uploads the firmware image to the FPC and the FPC restarts. When the FPC starts up, the configuration is reset to factory default settings and then synchronized by the management board. The FPC restarts again, rejoins the cluster, and is ready to process traffic.
4. To verify that the configuration of the FPC has been synchronized, enter the `diagnose sys confsync status | grep in_sy` command. The command output below shows an example of the synchronization status of some of the FPCs in an HA cluster of two FortiGate-6301F devices. The field `in_sync=1` indicates that the configuration of the FPC is synchronized.

   ```
   FPC6KFT018901327, Slave, uptime=615368.33, priority=19, slot_id=1:1, idx=1, flag=0x4, in_
   sync=1
   ```

```
F6KF31T018900143, Master, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_
sync=1
FPC6KFT018901372, Slave, uptime=615319.63, priority=20, slot_id=1:2, idx=1, flag=0x4, in_
sync=1
F6KF31T018900143, Master, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_
sync=1
FPC6KFT018901346, Slave, uptime=423.91, priority=21, slot_id=1:3, idx=1, flag=0x4, in_
sync=1
```

FPCs that are missing or that show `in_sync=0` are not synchronized. To synchronize an FPC that is not synchronized, log into the CLI of the FPC and restart it using the `execute reboot` command. If this does not solve the problem, contact Fortinet Support.

The example output also shows that the uptime of the FPC in slot 3 is lower than the uptime of the other FPCs, indicating that the FPC in slot 3 has recently restarted.

If you enter the `diagnose sys confsync status | grep in_sy` command before an FPC has completely restarted, it will not appear in the output. Also, the Security Fabric dashboard widget will temporarily show that it is not synchronized.

Installing FortiGate-6000 firmware from the BIOS after a reboot

A common method for resetting the configuration of a FortiGate involves installing firmware by restarting the FortiGate, interrupting the boot process, and using BIOS prompts to download a firmware image from a TFTP server. This process is also considered the best way to reset the configuration of your FortiGate.

Installing or upgrading FortiGate-6000 firmware from the BIOS after a reboot installs firmware on and resets the configuration of the management board only. FPCs will continue to operate with their current configuration and firmware build. The FortiGate-6000 system does not synchronize firmware upgrades that are performed from the BIOS. After you install firmware on the management board from the BIOS after a reboot, you must synchronize the new firmware build and configuration to the FPCs.

Use the following steps to upload firmware from a TFTP server to the management board. This procedure involves creating a connection between the TFTP server and one of the MGMT interfaces.

This procedure also involves connecting to the management board CLI using the FortiGate-6000 console port, rebooting the management board, interrupting the boot from the console session, and following BIOS prompts to install the firmware. During this procedure, the FortiGate-6000 will not be able to process traffic.

1. Set up a TFTP server and copy the firmware file to the TFTP server default folder.
2. Set up your network to allow traffic between the TFTP server and one of the management interfaces, (for example, MGMT1).
3. Using the console cable supplied with your FortiGate 6000, connect the console port on the FortiGate to the RS-232 port on your management computer.
4. Start a terminal emulation program on the management computer. Use these settings:
   Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.
5. Log in to the management board CLI.
6. To restart the management board, enter the `execute reboot` command.

7. When the management board starts up, follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.
8. To set up the TFTP configuration, press C.
9. Use the BIOS menu to set the following.Change settings only if required.
   `[P]: Set image download port`: MGMT1 (the connected MGMT interface)
   `[D]: Set DHCP mode`: Disabled
   `[I]: Set local IP address`: The IP address of the MGMT interface that you want to use to connect to the TFTP server. This address can be the same as the FortiGate-6000 management IP address and cannot conflict with other addresses on your network.
   `[S]: Set local Subnet Mask`: Set as required for your network.
   `[G]: Set local gateway`: Set as required for your network.
   `[V]: Local VLAN ID`: Should be set to `<none>`. (use -1 to set the Local VLAN ID to `<none>`.)
   `[T]: Set remote TFTP server IP address`: The IP address of the TFTP server.
   `[F]: Set firmware image file name`: The name of the firmware image file that you want to install.
10. To quit this menu, press Q.
11. To review the configuration, press R.
    To make corrections, press C and make the changes as required. When the configuration is correct, proceed to the next step.
12. To start the TFTP transfer, press T.
    The management board downloads the firmware image from the TFTP server and installs it on the management board. The management board then restarts with its configuration reset to factory defaults.
13. Once the management board restarts, verify that the correct firmware is installed.
    You can do this from the management board GUI dashboard or from the CLI using the `get system status` command.
14. Continue by Synchronizing the FPCs with the management board on page 21.

Synchronizing the FPCs with the management board

After you install firmware on the management board from the BIOS after a reboot, the firmware version and configuration of the management board will most likely not be synchronized with the FPCs. You can verify this from the management board CLI using the `diagnose sys confsync status | grep in_sy` command. The `in_sync=0` entries in the following example output for a FortiGate-6301F show that the management board (serial number ending in 143) is not synchronized with the FPCs.

```
diagnose sys confsync status | grep in_sy
FPC6KFT018901327, Slave, uptime=59.44, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Master, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901372, Slave, uptime=58.48, priority=20, slot_id=1:2, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Master, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901346, Slave, uptime=58.44, priority=21, slot_id=1:3, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Master, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901574, Slave, uptime=58.43, priority=22, slot_id=1:4, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Master, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901345, Slave, uptime=57.40, priority=23, slot_id=1:5, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Master, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901556, Slave, uptime=58.43, priority=24, slot_id=1:6, idx=1, flag=0x4, in_sync=0
F6KF31T018900143, Master, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
```

```
F6KF31T018900143, Master, uptime=119.72, priority=1, slot_id=1:0, idx=0, flag=0x0, in_sync=1
FPC6KFT018901327, Slave, uptime=59.44, priority=19, slot_id=1:1, idx=1, flag=0x4, in_sync=0
FPC6KFT018901345, Slave, uptime=57.40, priority=23, slot_id=1:5, idx=2, flag=0x4, in_sync=0
FPC6KFT018901346, Slave, uptime=58.44, priority=21, slot_id=1:3, idx=3, flag=0x4, in_sync=0
FPC6KFT018901372, Slave, uptime=58.48, priority=20, slot_id=1:2, idx=4, flag=0x4, in_sync=0
FPC6KFT018901556, Slave, uptime=58.43, priority=24, slot_id=1:6, idx=5, flag=0x4, in_sync=0
FPC6KFT018901574, Slave, uptime=58.43, priority=22, slot_id=1:4, idx=6, flag=0x4, in_sync=0
```

You can also verify the synchronization status from the management board Security Fabric dashboard widget.

To re-synchronize the FortiGate-6000, which has the effect of resetting all of the FPCs, re-install firmware on the management board.

You can also manually install firmware on each FPC from the BIOS after a reboot. This multi-step manual process is just as effective as installing the firmware for a second time on the management board to trigger synchronization to the FPCs, but takes much longer.

1. Log in to the management board GUI.
2. Install a firmware build on the management board from the GUI or CLI. The firmware build you install on the management board can either be the same firmware build or a different one.

   Installing firmware synchronizes the firmware build and configuration from the management board to the FPCs.
3. Check the synchronization status from the **Security Fabric** dashboard widget or using the `diagnose sys confsync status | grep in_sy` command. The following example FortiGate-6301F output shows that the management board is synchronized with all of the FPCs because each line includes `in_sync=1`.

```
diagnose sys confsync status | grep in_sy
FPC6KFT018901327, Slave, uptime=3773.96, priority=19, slot_id=1:1, idx=1, flag=0x4, in_
sync=1
F6KF31T018900143, Master, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_
sync=1
FPC6KFT018901372, Slave, uptime=3774.26, priority=20, slot_id=1:2, idx=1, flag=0x4, in_
sync=1
F6KF31T018900143, Master, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_
sync=1
FPC6KFT018901346, Slave, uptime=3774.68, priority=21, slot_id=1:3, idx=1, flag=0x4, in_
sync=1
F6KF31T018900143, Master, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_
sync=1
FPC6KFT018901574, Slave, uptime=3774.19, priority=22, slot_id=1:4, idx=1, flag=0x4, in_
sync=1
F6KF31T018900143, Master, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_
sync=1
FPC6KFT018901345, Slave, uptime=3773.59, priority=23, slot_id=1:5, idx=1, flag=0x4, in_
sync=1
F6KF31T018900143, Master, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_
sync=1
FPC6KFT018901556, Slave, uptime=3774.82, priority=24, slot_id=1:6, idx=1, flag=0x4, in_
sync=1
F6KF31T018900143, Master, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_
sync=1
F6KF31T018900143, Master, uptime=3837.25, priority=1, slot_id=1:0, idx=0, flag=0x0, in_
```

```
sync=1
FPC6KFT018901327, Slave, uptime=3773.96, priority=19, slot_id=1:1, idx=1, flag=0x24, in_
sync=1
FPC6KFT018901345, Slave, uptime=3773.59, priority=23, slot_id=1:5, idx=2, flag=0x24, in_
sync=1
FPC6KFT018901346, Slave, uptime=3774.68, priority=21, slot_id=1:3, idx=3, flag=0x24, in_
sync=1
FPC6KFT018901372, Slave, uptime=3774.26, priority=20, slot_id=1:2, idx=4, flag=0x24, in_
sync=1
FPC6KFT018901556, Slave, uptime=3774.82, priority=24, slot_id=1:6, idx=5, flag=0x24, in_
sync=1
FPC6KFT018901574, Slave, uptime=3774.19, priority=22, slot_id=1:4, idx=6, flag=0x24, in_
sync=1
```

Restarting the FortiGate-6000

To restart the FortiGate-6000, connect to the management board CLI and enter the `execute reboot` command. After you enter this command, the management board and all of the FPCs restart.

To restart an individual FPC, log in to the CLI of that FPC and run the `execute reboot` command.

Failover in a standalone FortiGate-6000

A FortiGate-6000 will continue to operate even if an FPC fails. If a failure occurs, sessions being processed by that FPC also fail. All new sessions are load balanced to the remaining FPCs. Sessions that were being processed by the failed FPC are restarted and load balanced to the remaining FPCs.

An FPC can fail because of a hardware malfunction, a software problem, or a power supply failure. The FortiGate-6000 includes three hot-swappable power supplies in a 2+1 redundant configuration. At least two of the power supplies must be operating to provide power to the FortiGate-6000. If only one power supply is operating, some of the FPCs will be shut down. The FortiGate-6000 will continue to operate but with reduced performance because fewer FPCs are operating.

You can't replace an FPC that fails because of a hardware failure. Instead, you should RMA the FortiGate-6000.

To show the status of the FPCs, use the `diagnose load-balance status` command. In the command output, if `Status Message` is `Running` the FPC is operating normally. The following example shows the status of FPCs, for a FortiGate-6301F:

```
diagnose load-balance status
============================================================================
MBD SN: F6KF313E17900032
  Master FPC Blade: slot-2

      Slot  1: FPC6KF3E17900200
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
```

```
Slot  2: FPC6KF3E17900201
  Status:Working   Function:Active
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  3: FPC6KF3E17900207
  Status:Working   Function:Active
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  4: FPC6KF3E17900219
  Status:Working   Function:Active
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  5: FPC6KF3E17900235
  Status:Working   Function:Active
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  6: FPC6KF3E17900169
  Status:Working   Function:Active
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
```

Changing the FortiGate-6301F and 6501F log disk and RAID configuration

The FortiGate-6301F and FortiGate-6501F both include two internal 1-TByte log disks. By default the disks are in a RAID-1 configuration. In the RAID-1 configuration you can use the disks for disk logging only. You can use the `execute disk raid` command to disable RAID and use one of the disks for disk logging and the other for other purposes such as disk caching. You can also change the RAID level to RAID-0. Changing the RAID configuration deletes all data from the disks and can disrupt disk logging so a best practice is set the RAID configuration when initially setting up the FortiGate-6301F or 6501F.

From the CLI you can use the following command to show disk status:

```
execute disk list
```

Use the following command to disable RAID:

```
execute disk raid disable
```

RAID is disabled, the disks are separated and formatted.

Use the following command to change the RAID level to RAID-0:

```
execute disk raid rebuild-level 0
```

The disks are formatted for RAID-0.

Use the following command to rebuild the current RAID partition:

```
execute disk raid rebuild
```

The RAID is rebuilt at the current RAID level.

Use the following command to show RAID status. The following command output shows the disks configured for RAID-1.

```
execute disk raid status
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1000GB

Disk 1: OK Used 953GB
Disk 2: OK Used 953GB
```

Packet sniffing for FPC and management board packets

From the management board CLI, you can access a VDOM and use the `diagnose sniffer packet` command to view or sniff packets processed by the FPCs for this VDOM. To use this command, log into the management board and edit a VDOM. The command output will include packets processed by all of the FPCs in the selected VDOM.

You can also use the `diagnose sniffer packet` command from an individual FPC to view packets processed by that FPC.

From the management board the command syntax is:

```
diagnose sniffer packet <interface> <protocol-filter> <verbose> <count> <timestamp> <frame-
     size> <slot>
```

Where:

`<interface>` the name of one or more interfaces on which to sniff for packets. Use `any` to sniff packets for all interfaces.

`<protocol-filter>` a filter to select the protocol for which to view traffic. This can be simple, such as entering `udp` to view UDP traffic or complex to specify a protocol, port, and source and destination interface and so on.

`<verbose>` the amount of detail in the output, and can be:

1. display packet headers only.
2. display packet headers and IP data.
3. display packet headers and Ethernet data (if available).
4. display packet headers and interface names.
5. display packet headers, IP data, and interface names.
6. display packet headers, Ethernet data (if available), and interface names.

`<count>` the number of packets to view. You can enter Ctrl-C to stop the sniffer before the count is reached.

`<timestamp>` the timestamp format, `a` for UTC time and `l` for local time.

<frame-size> the frame size that is printed before truncation. Defaults to the interface MTU.

`<slot>` the FPC(s) for which to view packets.

- To view packets for one FPC enter the slot number of the FPC.
- To view packets for more than one FPC, enter the slot numbers separated by commas. You can also include a range. For example, to view packets for the FPCs in slots 1, 2, 3, and 6 you can enter `1,2,3,6` or `1-3,6`.
- To view packets for all FPCs, enter `all`.

- If you leave out the <slot> option, you can use the diagnose sniffer options slot command to set whether management board packets appear or whether management board and FPC packets appear.

Using the diagnose sniffer options slot command

You can use the diagnose sniffer options slot command to control what the diagnose sniffer packet command displays if you don't include the <slot> option. The default diagnose sniffer options slot setting causes the diagnose sniffer packet command to display packets processed by all FPCs and by the management board.

You can use the following command to only display packets processed by the management board:

```
diagnose sniffer options slot current
```

Then the next time you enter the diagnose sniffer packet command and leave out the <slot> option, only packets from the management board appear in the command output.

Filtering out internal management traffic

The FortiGate-6000 includes internal interfaces that process internal management and synchronization communication between FortiGate-6000 components. Because this traffic uses internal interfaces, if you specify one or more interface names in the diagnose sniffer packet command this traffic is filtered out. However, if you sniff traffic on any interface, internal management traffic can appear in the diagnose sniffer packet command output.

The diagnose sniffer options filter-out-internal-pkts option if enabled (the default), filters out this internal management traffic. You can disable this option if you want to see the internal management traffic in the diagnose sniffer packet output.

Diagnose debug flow trace for FPC and management board activity

The diagnose debug flow trace output from the FortiGate-6000 management board CLI now displays debug data for the management board and for all of the FPCs. Each line of output begins with the name of the component that produced the output. For example:

```
diagnose debug enable
[FPC06]  id=20085 trace_id=2 func=resolve_ip6_tuple_fast line=4190 msg="vd-vlan:0 received a packet(proto=6,
3ff5::100:10001->4ff5::13:80) from vlan-port1."
[FPC07]  id=20085 trace_id=2 func=resolve_ip6_tuple_fast line=4190 msg="vd-vlan:0 received a packet(proto=6,
3ff5::100:10000->4ff5::11:80) from vlan-port1."
[FPC06]  id=20085 trace_id=2 func=resolve_ip6_tuple line=4307 msg="allocate a new session-000eb730"
[FPC07]  id=20085 trace_id=2 func=resolve_ip6_tuple line=4307 msg="allocate a new session-000eb722"
[FPC06]  id=20085 trace_id=2 func=vf_ip6_route_input line=1125 msg="find a route: gw-4ff5::13 via vlan-port2
err 0 flags 01000001"
```

Running FortiGate-6000 diagnose debug flow trace commands from an individual FPC CLI shows traffic processed by that FPC only. For example:

```
diagnose debug enable
[FPC02]  id=20085 trace_id=2 func=resolve_ip6_tuple_fast line=4190 msg="vd-vlan:0 received a packet(proto=6,
3ff5::100:10001->4ff5::28:80) from vlan-port1."
[FPC02]  id=20085 trace_id=2 func=resolve_ip6_tuple line=4307 msg="allocate a new session-000f00fb"
[FPC02]  id=20085 trace_id=2 func=vf_ip6_route_input line=1125 msg="find a route: gw-4ff5::28 via vlan-port2
```

```
err 0 flags 01000001"
[FPC02]  id=20085 trace_id=2 func=fw6_forward_handler line=345 msg="Check policy between vlan-port1 -> vlan-
port2"
```

NMI switch and NMI reset commands

When working with Fortinet Support to troubleshoot problems with your FortiGate-6000 you can use the front panel non-maskable interrupt (NMI) switch to assist with troubleshooting. Pressing this switch causes the software to dump management board registers and backtraces to the console. After the data is dumped, the management board restarts and traffic is temporarily blocked. The management board should restart normally and traffic can resume once the management board is up and running.

You can use the following command to dump registers and backtraces of one or more FPCs to the console. After the data is dumped, the FPC or FPCs reboot. While the FPCs are rebooting, traffic is distributed to the remaining FPCs. The FPCs should restart normally and traffic can resume once they are up and running.

```
execute load-balance slot nmi-reset <slot-number(s)>
```

Where `<slot-number(s)>` can be one or more FPC slot numbers or slot number ranges with no space and separated by commas. For example:

```
execute load-balance slot nmi-reset 1,3-4
```

Showing how the DP3 processor will load balance a session

You can use the following command to display the FPC slot that the DP3 processor will load balance a session to.

```
diagnose load-balance dp find session {normal | reverse | fragment | pinhole}
```

Normal and reverse sessions

For a `normal` or corresponding `reverse` session you can define the following:

```
{normal | reverse} <ip-protocol> <src-ip> {<src-port> | <icmp-type> | <icmp-typecode>} <dst-
      ip> {<dst-port> | <icmp-id>} [<x-vid>] [<x-cfi>] [<x-pri>]
```

Fragment packet sessions

For a session for `fragment` packets you can define the following:

```
fragment <ip-protocol> {<src-port> | <icmp-type> | <icmp-typecode>} <dst-ip> <ip-id> [<x-vid>]
      [<x-cfi>] [<x-pri>]
```

Pinhole sessions

For a `pinhole` sessions you can define the following:

```
pinhole <ip-protocol> <dst-ip> <dst-port> [<x-vid>] [<x-cfi>] [<x-pri>]
```

Normal session example output

For example, the following command shows that a new TCP session (protocol number 6) with source IP address 11.1.1.11, source port 53386, destination IP address 12.1.1.11, and destination port 22 would be sent to TCP slot 8 by the DP3 processor.

```
diagnose load-balance dp find session normal 6 11.1.1.11 53386 12.1.1.11 22
========================================================================
MBD SN: F6KF503E17900068
Primary Bin 9708928
New session to slot 8 (src-dst-ip-sport-dport)
```

Additional information about the session also appears in the command output in some cases.

Load balancing and flow rules

This chapter provides an overview of how FortiGate-6000 Session-Aware Load Balancing (SLBC) works and then breaks down the details and explains why you might want to change some load balancing settings.

For information about IPsec load balancing, see FortiGate-6000 IPsec VPN on page 42.

FortiGate-6000 SLBC works as follows.

1. SLBC attempts to match all incoming sessions with a configured flow rule (see Load balancing and flow rules on page 29). If a session matches a flow rule, the session is directed according to the action setting of the flow rule. Usually flow rules send traffic that can't be load balanced to a specific FPC.
2. TCP, UDP, SCTP, ICMP (IPv4 only) and ESP (IPv4 only) sessions that do not match a flow rule are directed to the DP3 processors.

   The DP3 processors distribute sessions to the FPCs according to the load balancing method set by the `dp-load-distribution-method` option of the `config load-balance setting` command.
3. All other sessions are sent to the primary (or master) FPC.

Setting the load balancing method

The FortiGate-6000 load balances or distributes sessions based on the load balancing method set by the following command:

```
config load-balance setting
   set dp-load-distribution-method {to-master | src-ip | dst-ip | src-dst-ip | src-ip-sport |
        dst-ip-dport | src-dst-ip-sport-dport}
end
```

The default load balancing method, `src-dst-ip-sport-dport`, distributes sessions across all FPCs according to their source and destination IP address, source port, and destination port. This load balancing method represents true session-aware load balancing. Session aware load balancing takes all session information into account when deciding where to send new sessions and where to send additional packets that are part of an already established session.

For information about the other load balancing methods, see config load-balance setting on page 74.

Flow rules for sessions that cannot be load balanced

Some traffic types cannot be load balanced. Sessions for traffic types that cannot be load balanced should normally be sent to the primary (or master) FPC by configuring flow rules for that traffic. You can also configure flow rules to send traffic that cannot be load balanced to specific FPCs.

Create flow rules using the `config load-balance flow-rule` command. The default configuration uses this command to send IKE, GRE, session helper, Kerberos, BGP, RIP, IPv4 and IPv6 DHCP, PPTP, BFD, IPv4 multicast and IPv6 multicast to the primary FPC. You can view the default configuration of the `config load-balance flow-rule` command to see how this is all configured. For example, the following configuration sends BGP source and destination sessions to the primary FPC:

```
config load-balance flow-rule
   edit 3
      set status enable
      set vlan 0
      set ether-type ip
      set protocol tcp
      set src-l4port 179-179
      set dst-l4port 0-0
      set tcp-flag any
      set action forward
      set forward-slot master
      set priority 5
      set comment "bgp src"
   next
   edit 4
      set status enable
      set vlan 0
      set ether-type ip
      set protocol tcp
      set src-l4port 0-0
      set dst-l4port 179-179
      set tcp-flag any
      set action forward
      set forward-slot master
      set priority 5
      set comment "bgp dst"
   end
```

See Default configuration for traffic that cannot be load balanced on page 35 for a listing of all of the default flow rules.

Determining which FPC is operating as the primary (master) FPC

You can use the `diagnose load-balance status` command to determine which FPC is operating as the primary FPC. The following example `diagnose load-balance status` output for a FortiGate-6300F shows that the FPC in slot 1 is the primary (master) FPC. The command output also shows the status of all of the FPCs in the FortiGate-6300F.

```
diagnose load-balance status
================================================================================
MBD SN: F6KF313E17900032
  Master FPC Blade: slot-1

     Slot  1: FPC6KF3E1790020
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
```

```
    Slot  2: FPC6KF3E17900201
      Status:Working   Function:Active
      Link:      Base: Up          Fabric: Up
      Heartbeat: Management: Good   Data: Good
      Status Message:"Running"
    Slot  3: FPC6KF3E17900207
      Status:Working   Function:Active
      Link:      Base: Up          Fabric: Up
      Heartbeat: Management: Good   Data: Good
      Status Message:"Running"
    Slot  4: FPC6KF3E17900219
      Status:Working   Function:Active
      Link:      Base: Up          Fabric: Up
      Heartbeat: Management: Good   Data: Good
      Status Message:"Running"
    Slot  5: FPC6KF3E17900235
      Status:Working   Function:Active
      Link:      Base: Up          Fabric: Up
      Heartbeat: Management: Good   Data: Good
      Status Message:"Running"
    Slot  6: FPC6KF3E17900169
      Status:Working   Function:Active
      Link:      Base: Up          Fabric: Up
      Heartbeat: Management: Good   Data: Good
      Status Message:"Running"
```

You can also determine which FPC is operating as the primary (master) FPC by hovering over the FPCs in the Security Fabric dashboard widget.

SSL VPN load balancing

The FortiGate-6000 does not support load balancing SSL VPN sessions terminated by the FortiGate-6000. The recommended configuration is to direct SSL VPN sessions terminated by the FortiGate-6000 to the primary FPC.

SSL VPN sessions are sessions from an SSL VPN client to your configured SSL VPN server listening port.

Using a FortiGate-6000 as an SSL VPN server requires you to manually add an SSL VPN load balance flow rule to configure the FortiGate-6000 to send all SSL VPN sessions to the primary (master) FPC. To match with the SSL VPN server traffic, the rule should include a destination port that matches the destination port of the SSL VPN server. A basic rule to allow SSL VPN traffic could be:

```
config load-balance flow-rule
   edit 0
      set status enable
      set ether-type ipv4
      set protocol tcp
      set dst-l4port 10443-10443
      set forward-slot master
      set comment "ssl vpn server to primary FPC"
   end
```

This flow rule matches all sessions sent to port 10443 (the default SSL VPN server listening port) and sends these sessions to the primary FPC. This should match all of your SSL VPN traffic if you are using the default SSL VPN server listening port (10443). This flow rule also matches all other sessions using 10443 as the destination port so all of this traffic is also sent to the primary FPC.

Adding the SSL VPN server IP address

You can add the IP address of the FortiGate-6000 interface that receives SSL VPN traffic to the SSL VPN flow rule to make sure that the flow rule only matches the traffic if SSL VPN clients connecting to the SSL VPN server. For example, if the IP address of the interface is 172.25.176.32 and the SSL VPN flow rule ID is 26:

```
config load-balance flow-rule
   edit 26
      set status enable
      set ether-type ipv4
      set protocol tcp
      set dst-addr-ipv4 172.25.176.32 255.255.255.255
      set dst-l4port 10443-10443
      set forward-slot master
      set comment "ssl vpn server to primary FPC"
   end
```

This flow rule will now only match SSL VPN sessions with 172.25.176.32 as the destination address and send all of these sessions to the primary FPC.

If you change the SSL VPN server listening port

If you have changed the SSL VPN server listening port to 20443, you can change the SSL VPN flow rule as follows. This example also sets the source interface to port12, which is the SSL VPN server interfaces, instead of adding the IP address of port12 to the configuration:

```
config load-balance flow-rule
   edit 26
      set status enable
      set ether-type ipv4
      set protocol tcp
      set src-interface port12
      set dst-l4port 20443-20443
      set forward-slot master
      set comment "ssl vpn server to primary FPC"
   end
```

FortiOS Carrier GTP load balancing

if you are operating a FortiGate-6000 system that is licensed for FortiOS Carrier (also called FortiCarrier), you can use the information in this section to optimize GTP performance. The commands and settings in this chapter only apply if your FortiGate-6000 has a FortiOS Carrier license.

Optimizing NPU GTP performance

You can use the following command to optimize GTP performance:

```
config system npu
   set gtp-enhance-mode enable
end
```

Enabling `gtp-enhance-mode` usually improves GTP performance.

GTP-C load balancing

By default and for the best GTP-C tunnel setup and throughput performance, FortiGate-6000 systems licensed for FortiOS Carrier load balance GTP-C traffic to all FPCs. Normally you should use this default configuration for optimum GTP-C performance.

If you want GTP-C traffic to only be processed by the primary (or master) FPC, you can edit the following flow rule and set `status` to `enable`. When enabled, this flow rule sends all GTP-C traffic to the primary FPC. Enabling this flow rule can reduce GTP performance, since all GTP-C tunnel setup sessions will be done by the primary FPC and not distributed among all of the FPCs.

```
config load-balance flow-rule
   edit 17
      set status enable
      set vlan 0
      set ether-type ipv4
      set src-addr-ipv4 0.0.0.0 0.0.0.0
      set dst-addr-ipv4 0.0.0.0 0.0.0.0
      set protocol udp
      set src-l4port 0-0
      set dst-l4port 2123-2123
      set action forward
      set forward-slot master
      set priority 5
      set comment "gtp-c to master blade"
   end
```

GTP-U load balancing

To load balance GTP-U traffic, in addition to enabling `gtp-enhance-mode`, you should enable the following option:

```
config load-balance setting
   set gtp-load-balance enable
end
```

Enabling this option load balances GTP-U sessions to all of the FPCs. GTP-U load balancing uses Tunnel Endpoint Identifiers (TEIDs) to identify and load balance sessions.

Adding a flow rule to support DHCP relay

The FortiGate-6000 default flow rules may not handle DHCP relay traffic correctly.

The default configuration includes the following flow rules for DHCP traffic:

```
config load-balance flow-rule
   edit 7
      set status enable
      set vlan 0
      set ether-type ipv4
      set src-addr-ipv4 0.0.0.0 0.0.0.0
      set dst-addr-ipv4 0.0.0.0 0.0.0.0
      set protocol udp
      set src-l4port 67-67
      set dst-l4port 68-68
      set action forward
      set forward-slot master
      set priority 5
      set comment "dhcpv4 server to client"
   next
   edit 8
      set status enable
      set vlan 0
      set ether-type ipv4
      set src-addr-ipv4 0.0.0.0 0.0.0.0
      set dst-addr-ipv4 0.0.0.0 0.0.0.0
      set protocol udp
      set src-l4port 68-68
      set dst-l4port 67-67
      set action forward
      set forward-slot master
      set priority 5
      set comment "dhcpv4 client to server"
   end
```

These flow rules handle traffic when the DHCP client sends requests to a DHCP server using port 68 and the DHCP server responds using port 67. However, if DHCP relay is involved, requests from the DHCP relay to the DHCP server and replies from the DHCP server to the DHCP relay both use port 67. If this DHCP relay traffic passes through the FortiGate-6000 you must add a flow rule similar to the following to support port 67 DHCP traffic in both directions:

```
config load-balance flow-rule
   edit 8
      set status enable
      set vlan 0
      set ether-type ipv4
      set src-addr-ipv4 0.0.0.0 0.0.0.0
      set dst-addr-ipv4 0.0.0.0 0.0.0.0
      set protocol udp
      set src-l4port 67-67
      set dst-l4port 67-67
      set action forward
      set forward-slot master
      set priority 5
      set comment "dhcpv4 relay"
   next
```

Default configuration for traffic that cannot be load balanced

The default `configure load-balance flow-rule` command contains the recommended default flow rules that control how the FortiGate-6000 handles traffic types that cannot be load balanced. All of the default flow rules identify the traffic type using the options available in the command and direct matching traffic to the primary (or master) FPC (`action` set to `forward` and `forward-slot` set to `master`). The default flow rules also include a comment that identifies the traffic type. Most of the flow rules in the default configuration are enabled and are intended to send common traffic types that cannot be load balanced to the primary FPC.

The default configuration also includes disabled flow rules for Kerberos and PPTP traffic. Normally, you would only need to enable these flow rules if you know that your FortGate will be handling these types of traffic.

Finally, the default configuration disables IPsec VPN flow rules because, by default, IPsec VPN load balancing is enabled using the following command:

```
config load-balance setting
   config ipsec-load-balance enable
end
```

If you disable IP sec VPN load balancing by setting `ipsec-load-balance` to `disable`, the FortiGate-6000 automatically enables the IPsec VPN flow rules and sends all IPsec VPN traffic to the primary FPC.

The CLI syntax below was created with the `show full configuration` command.

```
config load-balance flow-rule
    edit 1
        set status disable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 88-88
        set dst-l4port 0-0
        set action forward
        set forward-slot master
        set priority 5
        set comment "kerberos src"
    next
    edit 2
        set status disable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 88-88
        set action forward
        set forward-slot master
        set priority 5
        set comment "kerberos dst"
    next
    edit 3
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 179-179
        set dst-l4port 0-0
```

```
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp src"
    next
    edit 4
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 179-179
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp dst"
    next
    edit 5
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 520-520
        set dst-l4port 520-520
        set action forward
        set forward-slot master
        set priority 5
        set comment "rip"
    next
    edit 6
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 521-521
        set dst-l4port 521-521
        set action forward
        set forward-slot master
        set priority 5
        set comment "ripng"
    next
    edit 7
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 67-67
        set dst-l4port 68-68
        set action forward
        set forward-slot master
```

```
        set priority 5
        set comment "dhcpv4 server to client"
    next
    edit 8
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 68-68
        set dst-l4port 67-67
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 client to server"
    next
    edit 9
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 1723-1723
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp src"
    next
    edit 10
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1723-1723
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp dst"
    next
    edit 11
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 3784-3784
        set action forward
        set forward-slot master
        set priority 5
        set comment "bfd control"
    next
    edit 12
```

```
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 3785-3785
        set action forward
        set forward-slot master
        set priority 5
        set comment "bfd echo"
    next
    edit 13
        set status enable
        set vlan 0
        set ether-type ipv6
          set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 547-547
        set dst-l4port 546-546
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 server to client"
    next
    edit 14
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 546-546
        set dst-l4port 547-547
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 client to server"
    next
    edit 15
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 224.0.0.0 240.0.0.0
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 multicast"
    next
    edit 16
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
```

```
        set dst-addr-ipv6 ff00::/8
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 multicast"
    next
    edit 17
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 2123-2123
        set action forward
        set forward-slot master
        set priority 5
        set comment "gtp-c to master blade"
    next
    edit 18
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike"
    next
    edit 19
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike-natt dst"
    next
    edit 20
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol esp
```

```
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 esp"
    next
    edit 21
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike"
    next
    edit 22
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike-natt dst"
    next
    edit 23
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol esp
        set action forward
        set forward-slot master
        set priority   5
        set comment "ipv4 esp"
    next
    edit 24
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1000-1000
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
```

```
        set comment "authd http to master blade"
    next
    edit 25
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1003-1003
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd https to master blade"
    next
    edit 26
        set status enable
        set vlan 0
        set ether-type ip
        set protocol vrrp
        set action forward
        set forward-slot all
        set priority 6
        set comment "vrrp to all blades"
    next
end
```

FortiGate-6000 IPsec VPN

FortiOS 6.0 for FortiGate-6000 supports the following IPsec VPN features:

- Interface-based IPsec VPN (also called route-based IPsec VPN) is supported.
- Static routes can point at IPsec VPN interfaces and can be used for routing the traffic inside the IPsec VPN tunnel.
- Dynamic routing (RIP, OSPF, BGP) over IPsec VPN tunnels is supported.
- Remote networks with 16- to 32-bit netmasks are supported.
- Site-to-Site IPsec VPN is supported.
- Dialup IPsec VPN is supported. The FortiGate-6000 can be the dialup server or client.
- IPv4 clear-text traffic (IPv4 over IPv4 or IPv4 over IPv6) is supported.

FortiOS 6.0 for FortiGate-6000 does not support the following IPsec VPN features:

- Policy-based IPsec VPN is not supported. Only tunnel or interface mode IPsec VPN is supported.
- Policy routes cannot be used for communication over IPsec VPN tunnels.
- Remote networks with 0- to 15-bit netmasks are not supported. Remote networks with 16- to 32-bit netmasks are supported.
- IPv6 clear-text traffic (IPv6 over IPv4 or IPv6 over IPv6) is not supported.
- Load-balancing IPsec VPN tunnels to multiple FPCs is not supported. IPsec VPN load balancing should be disabled. By default, all IPsec VPN traffic is handled by the primary FPC.
- IPsec SA synchronization between HA peers is not supported. After an HA failover, IPsec VPN tunnels have to be re-initialized.

FortiGate-6000 IPsec VPN load balancing

Since the FortiGate-6000 does not support IPsec VPN load balancing, the following option should always be disabled:

```
config load-balance setting
   set ipsec-load-balance disable
end
```

Disabling IPv4 IPsec VPN load balancing in this way enables the following flow rules:

IPv4 IPsec flow rules with `ipsec-load-balance` disabled

```
    edit 21
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
```

```
        set priority 5
        set comment "ipv4 ike"
    next
    edit 22
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike-natt dst"
    next
    edit 23
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol esp
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 esp"
    next
```

These flow rules should generally handle all IPv4 IPsec VPN traffic. You can also adjust them or add your own flow rules if you have an IPv4 IPsec VPN setup that is not compatible with the default flow rules.

FortiGate-6000 high availability

FortiGate-6000 for FortiOS 6.0 supports the following types of HA operation:

- FortiGate Clustering protocol (FGCP)
- FortiGates Session Life Support Protocol (FGSP) (FortiGate-6000 FGSP HA on page 58)
- Virtual Router Redundancy Protocol (VRRP) (FortiGate-6000 VRRP HA on page 61)

New HA features and changes

- FortiGate Session Life Support Protocol (FGSP) (also called standalone session sync) support.
- The following HA session synchronization options are now supported for FGCP HA:

```
config system ha
   set session-pickup {disable | enable}
   set session-pickup-connectionless {disable | enable}
   set session-pickup-delay {disable | enable}
   set inter-cluster-session-sync {disable | enable}
end
```

- The following HA session synchronization options are now supported for FGSP HA:

```
config system ha
   set session-pickup {disable | enable}
   set session-pickup-connectionless {disable | enable}
   set session-pickup-expectation {disable | enable}
   set session-pickup-nat {disable | enable}
end
```

Introduction to FortiGate-6000 FGCP HA

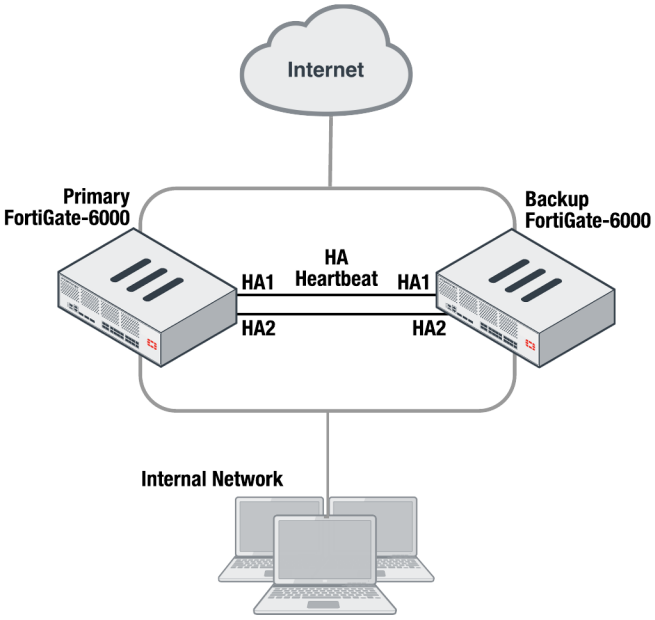
FortiGate-6000 supports active-passive FortiGate Clustering Protocol (FGCP) HA between two (and only two) identical FortiGate-6000s. You can configure FortiGate-6000 HA in much the same way as any FortiGate HA setup except that only active-passive HA is supported, and even though FortiGate-6000s are configured with VDOMS, virtual clustering is not supported.

You must use the 10Gbit HA1 and HA2 interfaces for HA heartbeat communication. The recommended HA heartbeat configuration is to use a cable to directly the HA1 interfaces of each FortiGate-6000 and another cable to directly connect the HA2 interfaces of each FortiGate-6000.

You can use switches to connect the HA heartbeat interfaces. Heartbeat packets are VLAN-tagged and you can configure the VLANs used. If you are using switches you must configure the switch interfaces in trunk mode and the switches must allow the VLAN-tagged packets.

As part of the FortiGate-6000 HA configuration, you assign each of the FortiGate-6000s in the HA cluster a chassis ID of 1 or 2. The chassis IDs just allow you to identify individual FortiGate-6000s and do not influence primary unit selection.

Example FortiGate-6000 HA configuration



In a FortiGate-6000 FGCP HA configuration, the primary (or master) FortiGate-6000 processes all traffic. The backup FortiGate-6000 operates in hot standby mode. The FGCP synchronizes the configuration, active sessions, routing information, and so on to the backup FortiGate-6000. If the primary FortiGate-6000 fails, traffic automatically fails over to the backup.

The FGCP selects the primary FortiGate-6000 based on standard FGCP primary unit selection:

- Connected monitored interfaces
- Age
- Device Priority
- Serial Number

In most cases and with default settings, if everything is connected and operating normally, the FortiGate-6000 with the highest serial number becomes the primary FortiGate-6000. You can set the device priority higher on one of the FortiGate-6000s if you want it to become the primary FortiGate-6000. You can also enable override along with setting a higher device priority to make sure the same FortiGate-6000 always becomes the primary FortiGate-6000.

Before you begin configuring HA

Before you begin:

- The FortiGate-6000s should be running the same FortiOS firmware version.
- Interfaces should be configured with static IP addresses (not DHCP or PPPoE).
- Register and apply licenses to each FortiGate-6000 before setting up the HA cluster. This includes licensing for FortiCare, IPS, AntiVirus, Web Filtering, Mobile Malware, FortiClient, FortiCloud, and additional virtual domains (VDOMs).

- Both FortiGate-6000s in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs.
- FortiToken licenses can be added at any time because they are synchronized to all cluster members.

On each FortiGate-6000, make sure the configurations of the FPCs are synchronized before starting to configure HA. You can use the following command to verify the configuration status of the FPCs. The following example shows the results from a FortiGate-6300F.

```
diagnose sys confsync showchsum | grep all
all: c0 68 d2 67 e1 23 d9 3a 10 50 45 c5 50 f1 e6 8e
all: c0 68 d2 67 e1 23 d9 3a 10 50 45 c5 50 f1 e6 8e
all: c0 68 d2 67 e1 23 d9 3a 10 50 45 c5 50 f1 e6 8e
all: c0 68 d2 67 e1 23 d9 3a 10 50 45 c5 50 f1 e6 8e
all: c0 68 d2 67 e1 23 d9 3a 10 50 45 c5 50 f1 e6 8e
all: c0 68 d2 67 e1 23 d9 3a 10 50 45 c5 50 f1 e6 8e
all: c0 68 d2 67 e1 23 d9 3a 10 50 45 c5 50 f1 e6 8e
```

If the FPCs are synchronized, the listed checksums should all be the same.

You can also use the following command to list the FPCs that are synchronized. The example output, for a FortiGate-6300F, shows all six FPCs have been configured for HA and added to the cluster.

```
diagnose sys confsync status | grep in_sync
F6KF313E17900031, Slave, uptime=232441.23, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
F6KF313E17900031, Slave, uptime=232441.23, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
F6KF313E17900031, Slave, uptime=232441.23, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
F6KF313E17900031, Slave, uptime=232441.23, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
F6KF313E17900031, Slave, uptime=232441.23, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
F6KF313E17900031, Master, uptime=232441.23, priority=1, slot_id=1:0, idx=0, flag=0x10, in_sync=1
F6KF313E17900031, Slave, uptime=232441.23, priority=2, slot_id=1:0, idx=0, flag=0x10, in_sync=1
FPC6KF3E17900209, Slave, uptime=231561.99, priority=24, slot_id=1:6, idx=6, flag=0x24, in_sync=1
FPC6KF3E17900215, Slave, uptime=231524.81, priority=22, slot_id=1:4, idx=7, flag=0x24, in_sync=1
FPC6KF3E17900217, Slave, uptime=232289.83, priority=120, slot_id=1:5, idx=8, flag=0x24, in_sync=1
FPC6KF3E17900229, Slave, uptime=232271.59, priority=118, slot_id=1:3, idx=10, flag=0x24, in_sync=1
FPC6KF3E17900230, Slave, uptime=232330.19, priority=116, slot_id=1:1, idx=11, flag=0x24, in_sync=1
FPC6KF3E17900291, Slave, uptime=232314.29, priority=117, slot_id=1:2, idx=13, flag=0x24, in_sync=1
```

In this command output `in_sync=1` means the FPC is synchronized with the management board and `in_sync=0` means the FPC is not synchronized.

Connect the HA1 and HA2 interfaces for HA heartbeat communication

HA heartbeat communication between FortiGate-6000s happens over the 10Gbit HA1 and HA2 interfaces. To set up HA heartbeat connections:

- Connect the HA1 interfaces of the two FortiGate-6000s together either with a direct cable connection, or using a switch.
- Connect the HA2 interfaces in the same way.

Heartbeat packets are VLAN packets with VLAN ID 999 and ethertype 9890. The MTU value for the HA1 and HA2 interfaces is 1500. You can use the following commands to change the HA heartbeat packet VLAN ID and ethertype values if required for your switches. You must change these settings on each FortiGate-6000. By default, the HA1 and HA2 interface heartbeat packets use the same VLAN IDs.

```
config system ha
```

```
   set hbdev-vlan-id <vlan>
   set hbdev-second-vlan-id <vlan>
   set ha-eth-type <eth-type>
end
```

Using separate connections for HA1 and HA2 is recommended for redundancy. If you are using switches, it is also recommended that these switches be dedicated to HA heartbeat communication and not used for other traffic.

If you use the same switch for both HA1 and HA2, separate the HA1 and HA2 traffic on the switch, enable trunk mode for the switch interfaces, and set the heartbeat traffic on the HA1 and HA2 Interfaces to have different VLAN IDs. For example, use the following command to set the heartbeat traffic on HA1 to use VLAN ID 4091 and the heartbeat traffic on HA2 to use VLAN ID 4092:

```
config system ha
   set hbdev-vlan-id 4091
   set hbdev-second-vlan-id 4092
end
```

Example FortiGate-6000 switch configuration

The switch that you use for connecting HA heartbeat interfaces does not have to support IEEE 802.1ad (also known as Q-in-Q, double-tagging). But the switch should be able to forward the double-tagged frames. Some switches will strip out the inner tag and Fortinet recommends avoiding these switches. FortiSwitch D and E series can correctly forward double-tagged frames.

This configuration is not required for FortiGate-6000 HA configurations if you have set up direct connections between the HA heartbeat interfaces.

This example shows how to configure a FortiGate-6000 to use different VLAN IDs for the HA1 and HA2 HA heartbeat interfaces and then how to configure two interfaces on a Cisco switch to allow HA heartbeat packets.

This example sets the native VLAN ID for both switch ports to 777. You can use any VLAN ID as the native VLAN ID as long as the native VLAN ID is not the same as the allowed VLAN ID.

1. On both FortiGate-6000s, enter the following command to use different VLAN IDs for the HA1 and HA2 interfaces. The command sets the ha1 VLAN ID to 4091 and the ha2 VLAN ID to 4092:

```
config system ha
   set hbdev ha1 50 ha2 100
   set hbdev-vlan-id 4091
   set hbdev-second-vlan-id 4092
end
```

2. Use the `get system ha status` command to confirm the VLAN IDs.

```
get system ha status
...
HBDEV stats:
 F6KF51T018900026(updated 4 seconds ago):
```

```
  ha1: physical/10000full, up, rx-bytes/packets/dropped/errors=54995955/230020/0/0,
tx=63988049/225267/0/0, vlan-id=4091
  ha2: physical/10000full, up, rx-bytes/packets/dropped/errors=54995955/230020/0/0,
tx=63988021/225267/0/0, vlan-id=4092
 F6KF51T018900022(updated 3 seconds ago):
  ha1: physical/10000full, up, rx-bytes/packets/dropped/errors=61237440/230023/0/0,
tx=57746989/225271/0/0, vlan-id=4091
  ha2: physical/10000full, up, rx-bytes/packets/dropped/errors=61238907/230023/0/0,
tx=57746989/225271/0/0, vlan-id=4092
...
```

3. Configure the Cisco switch interface that connects the HA1 interfaces to allow packets with a VLAN ID of 4091:

```
interface <name>
switchport mode trunk
switchport trunk native vlan 777
switchport trunk allowed vlan 4091
```

4. Configure the Cisco switch port that connects the HA2 interfaces to allow packets with a VLAN ID of 4092:

```
interface <name>
switchport mode trunk
switchport trunk native vlan 777
switchport trunk allowed vlan 4092
```

Basic FortiGate-6000 HA configuration

Use the following steps to set up HA between two FortiGate-6000s. To configure HA, you assign a chassis ID (1 and 2) to each of the FortiGate-6000s. These IDs allow the FGCP to identify the chassis and do not influence primary FortiGate selection. Before you start, determine which FortiGate-6000 should be chassis 1 and which should be chassis 2.

1. Set up HA heartbeat communication as described in Connect the HA1 and HA2 interfaces for HA heartbeat communication on page 46.
2. Log into the GUI or CLI of the FortiGate-6000 that will become chassis 1.
3. Use the following CLI command to change the host name. This step is optional, but setting a host name makes the FortiGate-6000 easier to identify after the cluster has formed.

```
config system global
   set hostname 6K-Chassis-1
end
```

   From the GUI you can configure the host name by going to **System > Settings** and changing the **Host name**.
4. Enter the following command to configure basic HA settings for the chassis 1 FortiGate-6000.

```
config system ha
   set group-id 6
   set group-name My-6K-cluster
   set mode a-p
   set hbdev ha1 50 ha2 100
   set chassis-id 1
   set password <password>
end
```

   From the GUI you can configure HA by going to **System > HA**. Set the **Mode** to **Active-Passive**, set the **Group Name**, add a **Password**, and set the **Heartbeat Interface Priority** for the heartbeat interfaces (HA1 and HA2). You must configure the chassis ID and group ID from the CLI.

5. If you are connecting the HA heartbeat interfaces together with a switch, change the HA heartbeat VLAN IDs, for example:
```
config system ha
   set hbdev-vlan-id 4091
   set hbdev-second-vlan-id 4092
end
```
6. Log into the chassis 2 FortiGate-6000 and configure its host name, for example:
```
config system global
   set hostname 6K-Chassis-2
end
```
From the GUI you can configure the host name by going to **System > Settings** and changing the **Host name**.
7. Enter the following command to configure basic HA settings. The configuration must be the same as the chassis 1 configuration, except for the chassis ID.
```
config system ha
   set group-id 6
   set group-name My-6K-cluster
   set mode a-p
   set hbdev ha1 50 ha2 100
   set chassis-id 2
   set password <password>
end
```
From the GUI you can configure HA by going to **System > HA**. Set the **Mode** to **Active-Passive**, set the **Group Name**, add a **Password**, and set the **Heartbeat Interface Priority** for the heartbeat interfaces (HA1 and HA2). You must configure the chassis ID and group ID from the CLI.
8. If you are connecting the HA heartbeat interfaces together with a switch, change the HA heartbeat VLAN IDs, for example:
```
config system ha
   set hbdev-vlan-id 4091
   set hbdev-second-vlan-id 4092
end
```
Once you save your configuration changes, if the HA heartbeat interfaces are connected, the FortiGate-6000s negotiate to establish a cluster. You may temporarily lose connectivity with the FortiGate-6000s as the cluster negotiates and the FGCP changes the MAC addresses of the FortiGate-6000 interfaces.
9. Log into the cluster and view the HA Status dashboard widget or enter the `get system ha status` command to confirm that the cluster has formed and is operating normally.

   If the cluster is operating normally, you can connect network equipment, add your configuration, and start operating the cluster.

Verifying that the cluster is operating normally

You view the cluster status from the HA Status dashboard widget, by going to **System > HA**, or by using the `get system ha status` command.

If the HA Status widget or the `get system ha status` command shows a cluster has not formed, check the HA heartbeat connections. They should be configured as described in Connect the HA1 and HA2 interfaces for HA heartbeat communication on page 46.

You should also review the HA configurations of the FortiGate-6000s. When checking the configurations, make sure both FortiGate-6000s have the same HA configuration, including identical HA group IDs, group names, passwords, and HA heartbeat VLAN IDs.

The following example FortiGate-6000 `get system ha status` output shows a FortiGate-6000 cluster that is operating normally. The output shows which FortiGate-6000 has become the primary (master) FortiGate-6000 and how it was chosen. You can also see CPU and memory use data, HA heartbeat VLAN IDs, and so on.

```
get system ha status
Master selected using:
HA Health Status: OK
Model: FortiGate-6000F
Mode: HA A-P
Group: 6
Debug: 0
Cluster Uptime: 0 days 12:42:5
Cluster state change time: 2019-02-24 16:26:30
    <2019/02/24 16:26:30> F6KF31T018900143 is selected as the master because it has the
largest value of serialno.
    ses_pickup: disable
override: disable
Configuration Status:
    F6KF31T018900143(updated 4 seconds ago): in-sync
    F6KF51T018900022 (updated 0 seconds ago): in-sync
System Usage stats:
    F6KF31T018900143(updated 4 seconds ago):
        sessions=198, average-cpu-user/nice/system/idle=1%/0%/0%/97%, memory=5%
    F6KF51T018900022 (updated 0 seconds ago):
        sessions=0, average-cpu-user/nice/system/idle=2%/0%/0%/96%, memory=6%
HBDEV stats:
    F6KF31T018900143(updated 4 seconds ago):
        ha1: physical/10000full, up, rx-bytes/packets/dropped/errors=227791977/902055/0/0,
tx=85589814/300318/0/0, vlan-id=4091
        ha2: physical/10000full, up, rx-bytes/packets/dropped/errors=227791977/902055/0/0,
tx=85589814/300318/0/0, vlan-id=4092
    F6KF51T018900022(updated 0 seconds ago):
        ha1: physical/10000full, up, rx-bytes/packets/dropped/errors=0/0/0/0,
tx=85067/331/0/0, vlan-id=4091
        ha2: physical/10000full, up, rx-bytes/packets/dropped/errors=947346/3022/0/0,
tx=206768/804/0/0, vlan-id=4092
Master: 6K-Chassis-1    , F6KF31T018900143, cluster index = 0
Slave : 6K-Chassis-2    , F6KF51T018900022, cluster index = 1
number of vcluster: 1
vcluster 1: work 10.101.11.20
Master: F6KF31T018900143, operating cluster index = 0
Slave : F6KF51T018900022, operating cluster index = 1
Chassis Status: (Local chassis ID: 2)
    Chassis ID 1: Slave Chassis
        Slot ID 1: Master Slot
        Slot ID 2: Slave Slot
    Chassis ID 2: Master Chassis
        Slot ID 1: Master Slot
        Slot ID 2: Slave Slot
```

Managing individual management boards and FPCs in HA mode

In some cases, you may want to connect to the management board or an individual FPC in one of the FortiGate-6000s in an HA cluster.

Connecting to chassis 1

You can connect to the management board and individual FPCs in chassis 1 using the same special port numbers as for a standalone FortiGate-6000 (see FortiGate-6000 special management port numbers on page 16).

FortiGate-6000 special management port numbers

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8000	44300	2300	2200	16100
Slot 1 (FPC01)	8001	44301	2301	2201	16101
Slot 2 (FPC02)	8002	44302	2302	2202	16102
Slot 3 (FPC03)	8003	44303	2303	2203	16103
Slot 4 (FPC04)	8004	44304	2304	2204	16104
Slot 5 (FPC05)	8005	44305	2305	2205	16105
Slot 6 (FPC06)	8006	44306	2306	2206	16106
Slot 7 (FPC07)	8007	44307	2307	2207	16107
Slot 8 (FPC08)	8008	44308	2308	2208	16108
Slot 9 (FPC09)	8009	44309	2309	2209	16109
Slot 10 (FPC10)	8010	44310	2310	2210	16110

Connecting to chassis 2

Different special port numbers are required to connect to the management board and individual FPCs in chassis 2. For the management board and for most FPCs, the special port number is the same as the special port number for chassis 1 with the number 2 as the second last digit. For example, if the management IP address is 1.1.1.1 you can browse to https://1.1.1.1:44323 to connect to the FPC in chassis 2 slot 3.

For the FPC in slot 10, include the number 30 as the second last and last digits. For example, to connect to the FPC in slot 10 browse to https://1.1.1.1:44330.

FortiGate-6000 special management port numbers (chassis 2)

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8020	44320	2320	2220	16120
Slot 1 (FPC01)	8021	44321	2321	2221	16121
Slot 2 (FPC02)	8022	44322	2322	2222	16122
Slot 3 (FPC03)	8023	44323	2323	2223	16123
Slot 4 (FPC04)	8024	44324	2324	2224	16124
Slot 5 (FPC05)	8025	44325	2325	2225	16125
Slot 6 (FPC06)	8026	44326	2326	2226	16126
Slot 7 (FPC07)	8027	44327	2327	2227	16127
Slot 8 (FPC08)	8028	44328	2328	2228	16128
Slot 9 (FPC09)	8029	44329	2329	2229	16129
Slot 10 (FPC10)	8030	44330	2330	2230	16130

HA cluster firmware upgrades

Both management boards and all of the FPCs in a FortiGate-6000 HA cluster run the same firmware image. You upgrade the firmware from the primary FortiGate-6000 management board.

If `uninterruptable-upgrade` and `session-pickup` are enabled, firmware upgrades should only cause a minimal traffic interruption. Use the following command to enable these settings; they are disabled by default. These settings are synchronized.

```
config system ha
   set uninterruptable-upgrade enable
   set session-pickup enable
end
```

When these settings are enabled, the primary FortiGate-6000 management board uploads firmware to the backup FortiGate-6000 management board. The backup management board uploads the firmware to all of the FPCs in the backup FortiGate-6000. Then the management board and all of the FPCs in the backup FortiGate-6000 upgrade their firmware, reboot, and resynchronize.

Then all traffic fails over to the backup FortiGate-6000 which becomes the new primary FortiGate-6000. Then the management board and the FPCs in the new backup FortiGate-6000 upgrade their firmware and rejoin the cluster. Unless override is enabled, the new primary FortiGate-6000 continues to operate as the primary FortiGate-6000.

Normally you would want to enable `uninterruptable-upgrade` to minimize traffic interruptions. But `uninterruptable-upgrade` does not have to be enabled. In fact, if a traffic interruption is not going to cause any problems, you can disable `uninterruptable-upgrade` so that the firmware upgrade process takes less time.

As well some firmware upgrades may not support `uninterruptable-upgrade`. For example, `uninterruptable-upgrade` may not be supported if the firmware upgrade also includes a DP3 processor firmware

upgrade. Make sure to review the release notes before running a firmware upgrade to verify whether or not enabling `uninterruptable-upgrade` is supported to upgrade to that version.

Distributed clustering

FortiGate-6000 HA supports separating the FortiGate-6000s in an HA cluster to different physical locations. Distributed FortiGate-6000 HA clustering (or geographically distributed FortiGate-6000 HA or geo clustering) can involve two FortiGate-6000s in different rooms in the same building, different buildings in the same location, or even different geographical sites such as different cities, countries, or continents.

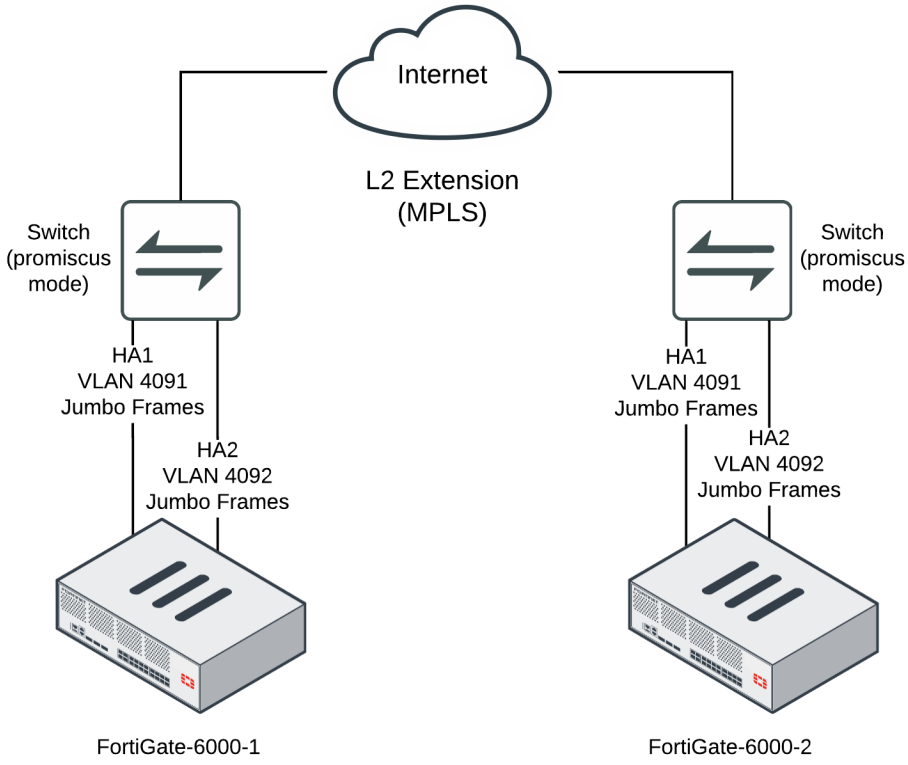
Just like any FortiGate-6000 HA configuration, distributed FortiGate-6000 HA requires heartbeat communication between the FortiGate-6000s over the HA1 and HA2 interfaces. In a distributed FortiGate-6000 HA configuration this heartbeat communication can take place over the internet or over other transmission methods including satellite linkups.

Most Data Center Interconnect (DCI) or MPLS-based solutions that support layer 2 extensions and VLAN tags between the remote data centers should also support HA heartbeat communication between the FortiGates in the distributed locations. Using VLANs and switches in promiscuous mode to pass all traffic between the locations can also be helpful.

You cannot change HA heartbeat IP addresses, so the heartbeat interfaces have to be able to communication over the same subnet.

The HA1 and HA2 interface traffic must be separated. You can do this by using separate channels for each interface or by configuring the HA1 and HA2 interfaces to use different VLANs.

Example FortiGate-6000 distributed clustering configuration



Because of the possible distance between sites, it may take a relatively long time for heartbeat packets to be transmitted between the FortiGate-6000s. This could lead to a split brain scenario. To avoid a split brain scenario you can modify heartbeat timing so that the cluster expects extra time between heartbeat packets. As a general rule, set the heartbeat failover time (`hb-interval`) to be longer than the max latency or round trip time (RTT). You could also increase the `hb-lost-threshold` to tolerate losing heartbeat packets if the network connection is less reliable.

In addition you could use different link paths for heartbeat packets to optimize HA heartbeat communication. You could also configure QoS on the links used for HA heartbeat traffic to make sure heartbeat communication has the highest priority.

For information about changing the heartbeat interval and other heartbeat timing related settings, see Modifying heartbeat timing on page 54.

Modifying heartbeat timing

If the FortiGate-6000s in the HA cluster do not receive heartbeat packets on time, the FortiGate-6000s in the HA configuration may each determine that the other FortiGate-6000 has failed. HA heartbeat packets may not be sent on time because of network issues. For example, if the HA1 and HA2 communications links between the FortiGate-6000s become too busy to handle the heartbeat traffic. Also, in a distributed clustering configuration the round trip time (RTT) between the FortiGate-6000s may be longer the expected time between heartbeat packets.

In addition, if the FortiGate-6000s becomes excessively busy, they may delay sending heartbeat packets.

Even with these delays, the FortiGate-6000 HA cluster can continue to function normally as long as the HA heartbeat configuration supports longer delays between heartbeat packets and more missed heartbeat packets.

You can use the following commands to configure heartbeat timing:

```
config system ha
   set hb-interval <interval_integer>
   set hb-lost-threshold <threshold_integer>
   set hello-holddown <holddown_integer>
end
```

Changing the heartbeat interval

The heartbeat interval is the time between sending HA heartbeat packets. The heartbeat interval range is 1 to 20 (100*ms). The heartbeat interval default is 2 (200 ms).

A heartbeat interval of 2 means the time between heartbeat packets is 200 ms. Changing the heartbeat interval to 5 changes the time between heartbeat packets to 500 ms (5 * 100ms = 500ms).

Use the following CLI command to increase the heartbeat interval to 10:

```
config system ha
   set hb-interval 10
end
```

Changing the lost heartbeat threshold

The lost heartbeat threshold is the number of consecutive heartbeat packets that a FortiGate-6000 does not receive before assuming that a failure has occurred. The default value of 6 means that if a FortiGate-6000 does not receive 6 heartbeat packets, it determines that the other FortiGate-6000 in the cluster has failed. The range is 1 to 60 packets.

The lower the `hb-lost-threshold`, the faster a FortiGate-6000 HA configuration responds when a failure occurs. However, sometimes heartbeat packets may not be received because the other FortiGate-6000 is very busy or because of network conditions. This can lead to a false positive failure detection. To reduce these false positives you can increase the `hb-lost-threshold`.

Use the following command to increase the lost heartbeat threshold to 12:

```
config system ha
   set hb-lost-threshold 12
end
```

Adjusting the heartbeat interval and lost heartbeat threshold

The heartbeat interval combines with the lost heartbeat threshold to set how long a FortiGate-6000 waits before assuming that the other FortiGate-6000 has failed and is no longer sending heartbeat packets. By default, if a FortiGate-6000 does not receive a heartbeat packet from a cluster unit for 6 * 200 = 1200 milliseconds or 1.2 seconds the FortiGate-6000 assumes that the other FortiGate-6000 has failed.

You can increase both the heartbeat interval and the lost heartbeat threshold to reduce false positives. For example, increasing the heartbeat interval to 20 and the lost heartbeat threshold to 30 means a failure will be assumed if no heartbeat packets are received after 30 * 2000 milliseconds = 60,000 milliseconds, or 60 seconds.

Use the following command to increase the heartbeat interval to 20 and the lost heartbeat threshold to 30:

```
config system ha
   set hb-lost-threshold 20
   set hb-interval 30
end
```

Changing the time to wait in the hello state

The hello state hold-down time is the number of seconds that a FortiGate-6000 waits before changing from the hello state to the work state. After a failure or when starting up, FortiGate-6000s in HA mode operate in the hello state to send and receive heartbeat packets, to find each other, and form a cluster. A FortiGate-6000 should change from the hello state to the work state after it finds the FortiGate-6000 to form a cluster with. If for some reason the FortiGate-6000s cannot find each other during the hello state, both FortiGate-6000s may assume that the other one has failed and each could form separate clusters of one FortiGate-6000. The FortiGate-6000s could eventually find each other and negotiate to form a cluster, possibly causing a network interruption as they re-negotiate.

One reason for a delay of the FortiGate-6000s finding each other could be the FortiGate-6000s are located at different sites or for some other reason communication is delayed between the heartbeat interfaces. If you find that your FortiGate-6000s leave the hello state before finding each other you can increase the time that they wait in the hello state. The hello state hold-down time range is 5 to 300 seconds. The hello state hold-down time default is 20 seconds.

Use the following command to increase the time to wait in the hello state to 1 minute (60 seconds):

```
config system ha
   set hello-holddown 60
end
```

Session failover (session-pickup)

Session failover means that after a failover, communication sessions resume on the new primary FortiGate-6000 with minimal or no interruption. Two categories of sessions need to be resumed after a failover:

- Sessions passing through the cluster
- Sessions terminated by the cluster

If sessions pickup is enabled, during cluster operation the primary FortiGate-6000 informs the backup FortiGate-6000 of changes to the primary FortiGate-6000 connection and state tables for TCP and UDP sessions passing through the cluster, keeping the backup FortiGate-6000 up-to-date with the traffic currently being processed by the cluster.

After a failover, the new primary FortiGate-6000 recognizes open sessions that were being handled by the cluster. The sessions continue to be processed by the new primary FortiGate-6000 and are handled according to their last known state.

Session-pickup has some limitations. For example, the FGCP does not support session failover for sessions being scanned by proxy-based security profiles. Session failover is supported for sessions being scanned by flow-based security profiles; however, flow-based sessions that fail over are not inspected after they fail over.

Sessions terminated by the cluster include management sessions (such as HTTPS connections to the FortiGate GUI or SSH connection to the CLI as well as SNMP and logging, and so on). Also included in this category are IPsec and SSL

VPN sessions terminated by the cluster and explicit proxy sessions. In general, whether or not session-pickup is enabled, these sessions do not failover and have to be restarted.

Enabling session pickup for TCP SCTP and connectionless sessions

To enable session synchronization for TCP and SCTP sessions, enter:

```
config system ha
   set session-pickup enable
end
```

Turning on session synchronization for TCP and SCTP sessions by enabling `session-pickup` also turns on session synchronization for connectionless sessions, such as ICMP and UDP, by enabling `session-pickup-connectionless`. You can now choose to reduce processing overhead by not synchronizing connectionless sessions if you don't need to. If you want to synchronize connectionless sessions you can enable `session-pickup-connectionless`.

When `session-pickup` is enabled, sessions in the primary FortiGate-6000 TCP and connectionless session tables are synchronized to the backup FortiGate-6000. As soon as a new session is added to the primary FortiGate-6000 session table, that session is synchronized to the backup FortiGate-6000. This synchronization happens as quickly as possible to keep the session tables synchronized.

If the primary FortiGate-6000 fails, the new primary FortiGate-6000 uses its synchronized session tables to resume all TCP and connectionless sessions that were being processed by the former primary FortiGate-6000 with only minimal interruption. Under ideal conditions, all sessions should be resumed. This is not guaranteed though and under less than ideal conditions some sessions may need to be restarted.

If session pickup is disabled

If you disable session pickup, the FortiGate-6000 HA cluster does not keep track of sessions and after a failover, active sessions have to be restarted or resumed. Most session can be resumed as a normal result of how TCP and UDP resumes communication after any routine network interruption.

The session-pickup setting does not affect session failover for sessions terminated by the cluster.

If you do not require session failover protection, leaving session pickup disabled may reduce CPU usage and reduce HA heartbeat network bandwidth usage. Also, if your FortiGate-6000 HA cluster is mainly being used for traffic that is not synchronized (for example, for proxy-based security profile processing) enabling session pickup is not recommended since most sessions will not be failed over anyway.

Reducing the number of sessions that are synchronized

If session pickup is enabled, as soon as new sessions are added to the primary unit session table they are synchronized to the other cluster units. Enable the session-pickup-delay CLI option to reduce the number of TCP sessions that are synchronized by synchronizing TCP sessions only if they remain active for more than 30 seconds. Enabling this option could greatly reduce the number of sessions that are synchronized if a cluster typically processes very many short duration sessions, which is typical of most HTTP traffic for example.

Use the following command to enable a 30 second session pickup delay:

```
config system ha
   set session-pickup-delay enable
end
```

Enabling session pickup delay means that if a failover occurs more sessions may not be resumed after a failover. In most cases short duration sessions can be restarted with only a minor traffic interruption. However, if you notice too many sessions not resuming after a failover you might want to disable this setting.

The `session-pickup-delay` option applies to TCP sessions only and does not apply to connectionless and SCTP sessions.

FortiGate-6000 FGSP HA

FortiGate-6000 supports the FortiGate Session Life Support Protocol (FGSP) (also called standalone session sync) HA to synchronize sessions among up to four FortiGate-6000s. All of the FortiGate-6000s in the FGSP cluster must be the same model and running the same firmware. All of the devices in an FGSP cluster must have their own network configuration (interface IPs, routing, and so on). FGSP synchronizes individual VDOM sessions. All of the devices in an FGSP cluster must include the VDOMs to be synchronized and for each device the VDOMs must have the same firewall configuration.

For details about FGSP for FortiOS 6.0, see: FortiOS 6.0 Handbook: FGSP.

FortiGate-6000 FGSP support has the following limitations:

- Configuration synchronization is currently not supported, you must configure all of the devices in the FGSP cluster separately or use FortiManager to keep key parts of the configuration, such as security policies, synchronized on the devices in the FGSP cluster.
- FortiGate-6000 FGSP can use the HA1 and HA2 interfaces for session synchronization. Using multiple interfaces is recommended for redundancy. To use these interfaces for FGSP, you must give them IP addresses and optionally set up routing for them. Ideally the session synchronization interfaces of each device in the FGSP cluster would be on the same network and that network would only be used for session synchronization traffic. However, you can configure routing to send session synchronization traffic between networks. NAT between session synchronization interfaces is not supported.
- Multiple VDOMs can be synchronized over the same session synchronization interface. You can also distribute synchronization traffic to multiple interfaces.
- FortiGate-6000 FGSP doesn't support setting up IPv6 session filters using the `config session-sync-filter` option.
- FGSP doesn't synchronize ICMP sessions when ICMP load balancing is set to `to-master`. If you want to synchronize ICMP sessions, set ICMP load balancing to either `src-ip`, `dst-ip`, or `src-dst-ip`. See ICMP load balancing on page 1 for more information.
- Asymmetric IPv6 SCTP traffic sessions are not supported. These sessions are dropped.
- Inter-cluster session synchronization, or FGSP between FGCP clusters, is not supported.
- FGSP IPsec tunnel synchronization is not supported.
- Fragmented packet synchronization is not supported.

FGSP session synchronization options

FortiGate-6000 FGSP supports the following HA session synchronization options:

```
config system ha
   set session-pickup {disable | enable}
   set session-pickup-connectionless {disable | enable}
   set session-pickup-expectation {disable | enable}
   set session-pickup-nat {disable | enable}
   set session-pickup-delay {disable | enable}
end
```

Some notes:

- The `session-pickup-expectation` and `session-pickup-nat` options only apply to FGSP HA. FGCP HA synchronizes NAT sessions when you enable `session-pickup`.
- The `session-pickup-delay` option applies to TCP sessions only and does not apply to connectionless and SCTP sessions.
- The `session-pickup-delay` option should not be used in FGSP topologies where the traffic can take an asymmetric path (forward and reverse traffic going through different FortiGates).

Enabling session synchronization

Enable `session-pickup` to synchronize sessions between the FortiGate-6000s in an FGSP cluster. Turning on session synchronization for TCP and SCTP sessions by enabling `session-pickup` also turns on session synchronization for connectionless protocol sessions, such as ICMP and UDP, by enabling `session-pickup-connectionless`. If you don't want to synchronize connectionless sessions, you can manually disable `session-pickup-connectionless`.

Synchronizing expectation sessions

Enable `session-pickup-expectation` to synchronize expectation sessions. FortiOS session helpers keep track of the communication of Layer-7 protocols such as FTP and SIP that have control sessions and expectation sessions. Usually the control sessions establish the link between server and client and negotiate the ports and protocols that will be used for data communications. The session helpers then create expectation sessions through the FortiGate for the ports and protocols negotiated by the control session.

The expectation sessions are usually the sessions that actually communicate data. For FTP, the expectation sessions transmit files being uploaded or downloaded. For SIP, the expectation sessions transmit voice and video data. Expectation sessions usually have a timeout value of 30 seconds. If the communication from the server is not initiated within 30 seconds the expectation session times out and traffic will be denied.

Synchronizing NAT sessions

Enable `session-pickup-nat` to synchronize NAT sessions in an FGSP cluster.

Synchronizing sessions older than 30 seconds

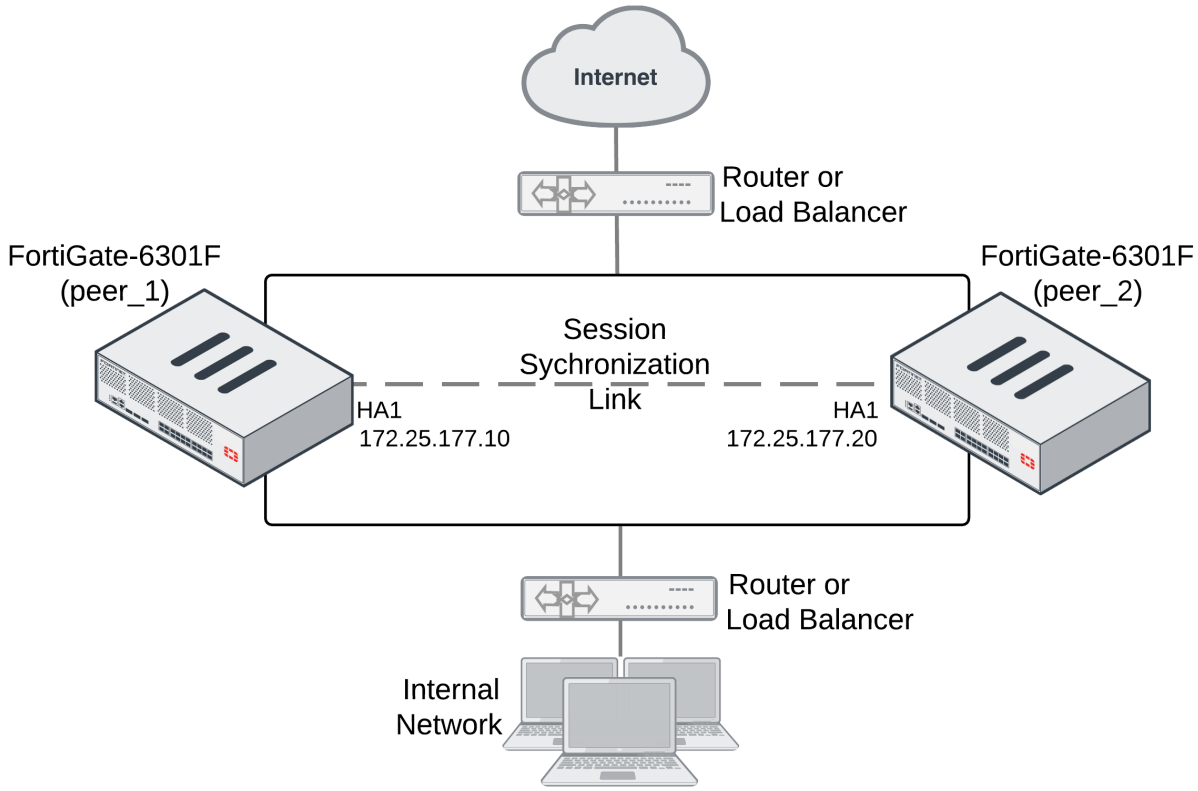
Enable `session-pickup-delay` to synchronize TCP sessions only if they remain active for more than 30 seconds. This option improves performance when `session-pickup` is enabled by reducing the number of TCP sessions that are synchronized. This option does not affect SCTP or connectionless sessions.

Example FortiGate-6000 FGSP configuration

This example shows how to configure an FGSP cluster to synchronize root VDOM sessions between two FortiGate-6301Fs. The example uses the HA1 interfaces of each FortiGate-6301F for session synchronization. The HA1 interfaces are connected to the 172.25.177.0/24 network.

Because configuration synchronization is not supported for FGSP you must set up both FortiGate-6000s with the same configuration, including the same VDOMs (although in this example, the root VDOM is synchronized) and the root VDOM must have the same firewall policies. The two FortiGate-6301Fs must have their own IP addresses and their own networking configuration. In addition, you can give the FortiGate-6301Fs different host names to make them easier to identify.

Example FortiGate-6000 FGSP configuration



1. Configure the routers or load balancers to send all sessions to peer_1.
2. Configure the routers or load balancers to send all traffic to peer_2 if peer_1 fails.
3. Give each FortiGate-6301F a different host name (in this case peer_1 and peer_2).
4. Configure network settings for each FortiGate-6301F to allow them to connect to their networks and route traffic.
5. Configure the root VDOM on each FortiGate-6301F with the same firewall policies.
6. Configure the HA1 interface of the peer_1 FortiGate-6301F with an IP address on the 172.25.177.0/24 network:

```
config system interface
   edit ha1
      set ip 172.25.177.10 255.255.255.0
```

```
   end
```

7. Configure the HA1 interface of the peer_2 FortiGate-6301F with an IP address on the 172.25.177.0/24 network:

```
config system interface
   edit ha1
      set ip 172.25.177.20 255.255.255.0
   end
```

8. On the peer_1 FortiGate-6301F, configure session synchronization for the root VDOM.

```
config system cluster-sync
   edit 0
      set peervd mgmt-vdom
      set peerip 172.25.177.20
      set syncvd root
   next
```

   Where, `peervd` will always be `mgmt-vdom`, the `peerip` is the IP address of the HA1 interface of the peer_2 FortiGate-6301F, and `syncvd` is the VDOM for which to synchronize sessions, in this case the root VDOM.

9. On the peer_2 FortiGate-6301F, configure session synchronization for the root VDOM.

```
config system cluster-sync
   edit 0
      set peervd mgmt-vdom
      set peerip 172.25.177.10
      set syncvd root
   next
```

   Where, `peervd` will always be `mgmt-vdom`, the `peerip` is the IP address of the HA1 interface of the peer_1 FortiGate-6301F, and `syncvd` is the VDOM for which to synchronize sessions, in this case the root VDOM.

FortiGate-6000 VRRP HA

The FortiGate-6000 platform supports the Virtual Router Redundancy Protocol (VRRP), allowing you to configure VRRP HA between FortiGate-6000 devices. You can also add a FortiGate-6000 to a VRRP domain with other VRRP routers.

To set up a FortiGate-6000 VRRP to provide HA for internet connectivity:

1. Add a virtual VRRP router to the internal interface to the FortiGate-6000(s) and routers to be in the VRRP domain.
2. Set the VRRP IP address of the domain to the internal network default gateway IP address.
3. Give one of the VRRP domain members the highest priority so it becomes the primary (or master) router and give the others lower priorities so they become backup routers.

During normal operation, the primary VRRP router sends outgoing VRRP routing advertisements. Both the primary and backup VRRP routers listen for incoming VRRP advertisements from other routers in the VRRP domain. If the primary router fails, the new primary router takes over the role of the default gateway for the internal network and starts sending and receiving VRRP advertisements.

For more information about FortiOS VRRP, see FortiGate Handbook: VRRP.

ICAP support

You can configure your FortiGate-6000 to use Internet Content Adaptation Protocol (ICAP) to offload processing that would normally take place on the FortiGate-6000 to a separate server specifically set up for the required specialized processing.

ICAP servers are focused on a specific function, for example:

- Ad insertion
- Virus scanning
- Content translation
- HTTP header or URL manipulation
- Language translation
- Content filtering

FortiGate-6000 supports ICAP without any special configuration. This includes using ICAP to offload decrypted SSL traffic to an ICAP server. FortiOS decrypts the content stream before forwarding it to the ICAP server.

For more information about FortiOS support for ICAP, see ICAP support.

Example ICAP configuration

ICAP is available for VDOMs operating in proxy mode. You can enable proxy mode from the **Global** GUI by going to **System > VDOM**, editing the VDOM for which to configure ICAP, and setting **Inspection Mode** to **Proxy**.

Then go to the VDOM, and go to **System > Feature Visibility** and enable **ICAP**.

From the CLI you can edit the VDOM, enable proxy inspection mode and enable ICAP. You can only enable ICAP from `config system settings` if proxy mode is already enabled.

```
config vdom
   edit VDOM-2
      config system settings
         set inspection-mode proxy
      end
      config system settings
         set gui-icap enable
      end
```

From the GUI you can add an ICAP profile by going to **Security Profiles > ICAP** and selecting **Create New** to create a new ICAP profile.

From the CLI you can use the following command to create an ICAP profile:

```
config icap profile
   edit "default"
   next
   edit "icap-test-profile"
      set request enable
      set response enable
      set request-server "icap-test"
      set response-server "icap-test"
      set request-failure bypass
```

```
      set response-failure bypass
      set request-path "echo"
      set response-path "echo"
   end
```

From the GUI you can add an ICAP serve by going to **Security Profiles > ICAP Servers** and selecting **Create New** to created a new ICAP server.

From the CLI you can use the following command to create an ICAP server:

```
config icap server
   edit "icap-test"
      set ip-address 10.98.0.88
      set max-connections 1000
   end
```

Then create a firewall policy for the traffic to be sent to the ICAP server and include the ICAP profile.

```
config firewall policy
   edit 4
      set name "any-any"
      set uuid f4b612d0-2300-51e8-f15f-507d96056a96
      set srcintf "1-C1/5" "1-C1/6"
      set dstintf "1-C1/6" "1-C1/5"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set logtraffic all
      set av-profile "default"
      set icap-profile "icap-test-profile"
      set profile-protocol-options "default"
      set ssl-ssh-profile "deep-inspection"
   end
```

SSL mirroring support

You can configure your FortiGate-6000 to "mirror" or send a copy of traffic decrypted by SSL inspection to one or more interfaces so that the traffic can be collected by a raw packet capture tool for archiving or analysis.

Decryption, storage, inspection, and use decrypted content is subject to local privacy rules. Use of these features could enable malicious users with administrative access to your FortiGate to harvest sensitive information submitted using an encrypted channel.

For more information about FortiOS support for SSL mirroring, see Mirroring SSL inspected traffic,

Example SSL mirroring configuration

SSL mirroring is available for VDOMs operating in flow mode. You can enable flow mode from the **Global** GUI by going to **System > VDOM**, editing the VDOM for which to configure SSL mirroring , and setting **Inspection Mode** to **Flow-based**.

From the CLI you can edit the VDOM and enable flow inspection mode.

```
config vdom
   edit mirror-vdom
      config system settings
         set inspection-mode flow
      end
```

To enable SSL mirroring, add a firewall policy to accept the traffic that you want to be mirrored. In the policy, enable the `SSL-mirror` option and set `ssl-mirror-intf` to the interface to which to send decrypted packets.

```
config firewall policy
   edit 4
      set name "ssl-mirror-example"
      set uuid f4b612d0-2300-51e8-f15f-507d96056a96
      set srcintf "port10"
      set dstintf "port11"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set logtraffic all
      set ssl-mirror enable
      set ssl-mirror-intf "port20"
      set ips-sensor "default"
      set application-list "default"
      set profile-protocol-options "default"
      set ssl-ssh-profile "deep-inspection"
   end
```

You can use the following command from an FPC CLI to verify the mirrored traffic:

```
diagnose sniffer packet port20 'port 443' -c 50
interfaces=[port20]
filters=[port 443]
pcap_lookupnet: port20: no IPv4 address assigned
0.440714 8.1.1.69.18478 -> 9.2.1.130.443: syn 582300852
0.440729 9.2.1.130.443 -> 8.1.1.69.18478: syn 3198605956 ack 582300853
0.440733 8.1.1.69.18478 -> 9.2.1.130.443: ack 3198605957
0.440738 8.1.1.69.18478 -> 9.2.1.130.443: psh 582300853 ack 3198605957
0.441450 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198605957 ack 582301211
0.441535 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198607351 ack 582301211
0.441597 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198608747 ack 582301211
0.441636 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198610143 ack 582301211
0.441664 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198611539 ack 582301211
0.441689 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198612935 ack 582301211
0.441715 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198614331 ack 582301211
0.441739 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198615727 ack 582301211
0.441764 9.2.1.130.443 -> 8.1.1.69.18478: psh 3198617123 ack 582301211
```

FortiGate-6000 v6.0.4 special features and limitations

This section describes special features and limitations for FortiGate-6000 v6.0.4.

Remote console limitations

Some console input may not function as expected. For example, when remotely connecting to an FPC console using Telnet, when viewing the BIOS menu, pressing the H key to display BIOS menu help does not always work as expected.

Default management VDOM

By default the FortiGate-6000 configuration includes a management VDOM named mgmt-vdom. The ha1, ha2, mgmt1, mgmt2, and mgmt3 interfaces are in mgmt-vdom and all other interfaces are in the root VDOM. For the FortiGate-6000 system to operate normally, mgmt-vdom must always be the management VDOM. You also must not remove interfaces from this VDOM. You can change the IP addresses of the interfaces in mgmt-vdom, allow the required management services, and add routes as required for management traffic.

You have full control over the configurations of other FortiGate-6000 VDOMs.

Default Security Fabric configuration

The FortiGate-6000 uses the Security Fabric for communication and synchronization between the management board and FPCs. Changing the default Security Fabric configuration could disrupt this communication and affect system performance.

Default Security Fabric configuration:

```
config system csf
   set status enable
   set configuration-sync local
   set management-ip 0.0.0.0
   set management-port 0
end
```

For the FortiGate-6000 to operate normally, you must not change the Security Fabric configuration.

Maximum number of LAGs

FortiGate-6000 systems support up to 16 link aggregation groups (LAGs). This includes both normal link aggregation groups and redundant interfaces.

Firewall

TCP or UDP sessions with NAT enabled that are expected to be idle for more than the distributed processing normal TCP timer (which is 3605 seconds) will timeout. If you encounter this problem you can use the following command to increase the TCP timer:

```
config system global
   set dp-tcp-normal-timer <timer>
end
```

IP Multicast

IPv4 and IPv6 Multicast traffic is only sent to the primary FPC. This is controlled by the following configuration:

```
config load-balance flow-rule
   edit 15
      set status enable
      set vlan 0
      set ether-type ipv4
      set src-addr-ipv4 0.0.0.0 0.0.0.0
      set dst-addr-ipv4 224.0.0.0 240.0.0.0
      set protocol any
      set action forward
      set forward-slot master
      set priority 5
      set comment "ipv4 multicast"
   next
   edit 16
      set status enable
      set vlan 0
      set ether-type ipv6
      set src-addr-ipv6 ::/0
      set dst-addr-ipv6 ff00::/8
      set protocol any
      set action forward
      set forward-slot master
      set priority 5
      set comment "ipv6 multicast"
   end
```

High Availability

Only the HA1 and HA2 interfaces are used for the HA heartbeat communication. For information on how to set up HA heartbeat communication using the HA1 and HA2 interfaces, see Connect the HA1 and HA2 interfaces for HA heartbeat communication on page 46.

The following FortiOS HA features are not supported or are supported differently by FortiGate-6000 v6.0.4:

- Active-active HA is not supported.
- The range for the HA `group-id` is 0 to 31.
- Failover logic for FortiGate-6000 v6.0.4 HA is the same as FGCP for other FortiGate clusters.
- HA heartbeat configuration is specific to FortiGate-6000 systems and differs from standard HA.

FortiOS features that are not supported by FortiGate-6000 v6.0.4

The following mainstream FortiOS 6.0.4 features are not supported by the FortiGate-6000 v6.0.4:

- SD-WAN (because of known issues)
- EMAC-VLANs (because of known issues)
- HA dedicated management interfaces
- Hardware switch
- Switch controller
- WiFi controller
- IPv4 over IPv6, IPv6 over IPv4, IPv6 over IPv6 features
- GRE tunneling is only supported after creating a load balance flow rule, for example:

```
config load-balance flow-rule
  edit 0
     set status enable
     set vlan 0
     set ether-type ip
     set protocol gre
     set action forward
     set forward-slot master
     set priority 3
  end
```

- Only the FortiGate-6301F and the FortiGate-6501F support hard disk features such as WAN optimization, web caching, explicit proxy content caching, disk logging, and GUI-based packet sniffing.
- The FortiGate-6000 platform, including the FortiGate-6301F and the FortiGate-6501F does not support quarantining files to the internal hard disks. Instead you must set the quarantine function to quarantine files to FortiAnalyzer.
- The management interfaces (mgmt1-3) do not support device detection for the networks they are connected to.
- The FortiGate-6000 does not support configuring dedicated management interfaces using the `config system dedicated-mgmt` command or by enabling the `dedicated-to management` interface option.

IPsec VPN tunnels terminated by the FortiGate-6000

For a list of new FortiOS 6.0.4 FortiGate-6000 IPsec VPN features and a list of IPsec VPN features not supported by FortiOS 6.0.4 FortiGate-6000 IPsec VPN, see FortiGate-6000 IPsec VPN on page 42.

SSL VPN

Sending all SSL VPN sessions to the primary (master) FPC is recommended. You can do this by:

- Creating a flow rule that sends all sessions that use the SSL VPN destination port and IP address to the primary FPC.
- Creating flow rules that send all sessions that use the SSL VPN IP pool addresses to the primary FPC.

SSL VPN can't listen on LACP LAG interfaces. This limitation will be fixed in a future release.

For more information about FortiGate-7000 SSL VPN support, see SSL VPN load balancing on page 31.

Traffic shaping

You can only configure traffic shaping from the CLI. Each FPC applies traffic shaping quotas independently. Traffic is first load balanced to the FPCs and then traffic shaping is applied by the FPC to the traffic load balanced to it.This may result in traffic shaping allowing more traffic than expected.

DDoS quotas

Each FPC applies DDoS quotas independently. Traffic is first load balanced to the FPCs and then DDoS quotas are applied by the FPC to the traffic load balanced to it. This may result in DDoS quotas being less effective than expected.

FortiGuard Web filtering and Spam filtering

The FortiGate-6000 sends all FortiGuard web filtering and spam filtering rating queries through a management interface from the management VDOM.

Log messages include a slot field

An additional "slot" field has been added to log messages to identify the FPC that generated the log.

Special notice for new deployment connectivity testing

Only the management board can successfully ping external IP addresses. During a new deployment, while performing connectivity testing from the Fortigate-6000, make sure to run `execute ping` tests from the management board and not from an FPC. See Using data interfaces for management traffic on page 15 for information about changes to this limitation.

FortiGate-6000 config CLI commands

This chapter describes the following FortiGate-6000 load balancing configuration commands:

config load-balance flow-rule

Use this command to create flow rules that add exceptions to how matched traffic is processed. You can use flow rules to match a type of traffic and control whether the traffic is forwarded or blocked. And if the traffic is forwarded, you can specify whether to forward the traffic to a specific slot or slots. Unlike firewall policies, load-balance rules are not stateful so for bi-directional traffic, you may need to define two flow rules to match both traffic directions (forward and reverse).

Syntax

```
config load-balance flow-rule
   edit <id>
      set status {disable | enable}
      set src-interface <interface-name> [<interface-name>...]
      set vlan <vlan-id>
      set ether-type {any | arp | ip | ipv4 | ipv6}
      set src-addr-ipv4 <ip4-address> <netmask>
      set dst-addr-ipv4 <ip4-address> <netmask>
      set src-addr-ipv6 <ip6-address> <netmask>
      set dst-addr-ipv6 <ip6-address> <netmask>
      set protocol {any | icmp | icmpv6 | tcp | udp | igmp | sctp | gre | esp | ah | ospf | pim
           | vrrp}
      set src-l4port <start>[-<end>]
      set dst-l4port <start>[-<end>]
      set icmptype <type>
      set icmpcode <type>
      set tcp-flag {any | syn | fin | rst}
      set action {forward | mirror-ingress | stats | drop}
      set mirror-interface <interface-name>
      set forward-slot {master | all | load-balance | <FPC#>}
      set priority <number>
      set comment <text>
   end
```

status {disable | enable}

Enable or disable this flow rule. New flow rules are disabled by default.

src-interface <interface-name> [interface-name>...]

Optionally add the names of one or more front panel interfaces accepting the traffic to be subject to the flow rule. If you don't specify a `src-interface`, the flow rule matches traffic received by any interface.

If you are matching VLAN traffic, select the interface that the VLAN has been added to and use the `vlan` option to specify the VLAN ID of the VLAN interface.

vlan <vlan-id>

If the traffic matching the rule is VLAN traffic, enter the VLAN ID used by the traffic. You must set `src-interface` to the interface that the VLAN interface is added to.

ether-type {any | arp | ip | ipv4 | ipv6}

The type of traffic to be matched by the rule. You can match any traffic (the default) or just match ARP, IP, IPv4 or IPv6 traffic.

{src-addr-ipv4 | dst-addr-ipv4} <ipv4-address> <netmask>

The IPv4 source and destination address of the IPv4 traffic to be matched. The default of `0.0.0.0 0.0.0.0` matches all IPv4 traffic. Available if `ether-type` is set to `ipv4`.

{src-addr-ipv6 | dst-addr-ipv6} <ip-address> <netmask>

The IPv6 source and destination address of the IPv6 traffic to be matched. The default of `::/0` matches all IPv6 traffic. Available if `ether-type` is set to `ipv6`.

protocol {any | icmp | icmpv6 | tcp | udp | igmp | sctp | gre | esp | ah | ospf | pim | vrrp}

If `ether-type` is set to `ip`, `ipv4`, or `ipv6`, specify the protocol of the IP, IPv4, or IPv6 traffic to match the rule. The default is `any`.

Option	Protocol number
icmp	1
icmpv6	58
tcp	6
udp	17
igmp	2
sctp	132
gre	47

Option	Protocol number
esp	50
ah	51
ospf	89
pim	103
vrrp	112

{src-l4port | dst-l4port} <start>[-<end>]

Specify a layer 4 source port range and destination port range. This option appears when `protocol` is set to `tcp` or `udp`. The default range is 0-0, which matches all ports. You don't have to enter a range to match just one port. For example, to set the source port to 80, enter `set src-l4port 80`.

icmptype <type>

Specify an ICMP type number in the range of 0 to 255. The default is 255. This option appears if `protocol` is set to `icmp`. For information about ICMP type numbers, see Internet Control Message Protocol (ICMP) Parameters.

icmpcode <type>

If the ICMP type also includes an ICMP code, you can use this option to add that ICMP code. The ranges is 0 to 255. The default is 255. This option appears if `protocol` is set to `icmp`. For information about ICMP code numbers, see Internet Control Message Protocol (ICMP) Parameters.

tcp-flag {any | syn | fin | rst}

Set the TCP session flag to match. The `any` setting (the default) matches all TCP sessions. You can add specific flags to only match specific TCP session types.

action {forward | mirror-ingress | stats | drop}

The action to take with matching sessions. They can be dropped, forwarded to another destination, or you can record statistics about the traffic for later analysis. You can combine two or three settings in one command for example, you can set `action` to both `forward` and `stats` to forward traffic and collect statistics about it. Use `append` to append additional options.

The default action is `forward`, which forwards packets to the specified `forward-slot`.

The `mirror-ingress` option copies (mirrors) all ingress packets that match this flow rule and sends them to the interface specified with the `mirror-interface` option.

set mirror-interface <interface-name>

The name of the interface to send packets matched by this flow-rule to when `action` is set to `mirror-ingress`.

forward-slot {master | all | load-balance | <FPC#>}

The slot that you want to forward the traffic that matches this rule to.

Where:

`master` forwards traffic to the primary FPC.

`all` means forward the traffic to all FPCs.

`load-balance` means forward this traffic to the DP processors that then use the default load balancing configuration to handle this traffic.

`<FPC#>` forward the matching traffic to a specific FPC. For example, FPC3 is the FPC in slot 3.

priority <number>

Set the priority of the flow rule in the range 1 (highest priority) to 10 (lowest priority). Higher priority rules are matched first. You can use the priority to control which rule is matched first if you have overlapping rules.

The default priority is 5.

comment <text>

Optionally add a comment that describes the flow rule.

config load-balance setting

Use this command to set a wide range of load balancing settings.

```
config load-balance setting
   set slbc-mgmt-intf {mgmt1 | mgmt2 | mgmt3)
   set max-miss-heartbeats <heartbeats>
   set max-miss-mgmt-heartbeats <heartbeats>
   set weighted-load-balance {disable | enable}
   set ipsec-load-balance {disable | enable}
   set gtp-load-balance {disable | enable}
   set dp-keep-assist-sessions {disable | enable}
   set dp-load-distribution-method {to-master | src-ip | dst-ip | src-dst-ip | src-ip-sport |
        dst-ip-dport | src-dst-ip-sport-dport}
   set dp-icmp-distribution-method {to-master | src-ip | dst-ip | src-dst-ip | derived}
   set dp-session-table-type {vdom-based | intf-vlan-based}
      config workers
         edit 3
            set status {disable | enable}
            set weight <weight>
         end
end
```

slbc-mgmt-intf {mgmt1 | mgmt2 | mgmt3)

Selects the interface used for management connections. The default is `mgmt1`. The IP address of this interface becomes the IP address used to enable management access to individual FPCs using special administration ports as described in Managing individual FPCs on page 16. To manage individual FPCs, this interface must be connected to a network.

max-miss-heartbeats <heartbeats>

Set the number of missed heartbeats before an FPC is considered to have failed. If a failure occurs, the DP3 processor will no longer load balance sessions to the FPC.

The time between heartbeats is 0.2 seconds. Range is 3 to 300. A value of 3 means 0.6 seconds, 20 (the default) means 4 seconds, and 300 means 60 seconds.

max-miss-mgmt-heartbeats <heartbeats>

Set the number of missed management heartbeats before a FPC is considering to have failed. If a failure occurs, the DP3 processor will no longer load balance sessions to the FPC.

The time between management heartbeats is 1 second. Range is 3 to 300 heartbeats. The default is 10 heartbeats.

weighted-load-balance {disable | enable}

Enable weighted load balancing depending on the slot (or worker) weight. Use `config workers` to set the weight for each slot or worker.

ipsec-load-balance {disable | enable}

Enable or disable IPsec VPN load balancing.

By default IPsec VPN load balancing is enabled and the flow rules listed below are disabled. The FortiGate-6000 directs IPsec VPN sessions to the DP3 processors which load balance them among the FPCs.

Default IPsec VPN flow-rules

```
    edit 21
        set status disable
        set ether-type ipv4
        set protocol udp
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set comment "ipv4 ike"
    next
    edit 22
        set status disable
        set ether-type ipv4
```

```
        set protocol udp
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set comment "ipv4 ike-natt dst"
    next
    edit 23
        set status disable
        set ether-type ipv4
        set protocol esp
        set action forward
        set forward-slot master
        set comment "ipv4 esp"
    next
```

If IPsec VPN load balancing is enabled, the FortiGate-6000 will drop IPsec VPN sessions traveling between two IPsec tunnels because the two IPsec tunnels may be terminated on different FPCs. If you have traffic entering the FortiGate-6000 from one IPsec VPN tunnel and leaving the FortiGate-6000 out another IPsec VPN tunnel you need to disable IPsec load balancing. Disabling IPsec VPN load balancing enables the default IPsec VPN flow-rules.

gtp-load-balance {disable | enable}

Enable GTP load balancing. If GTP load balancing is enabled, Tunnel Endpoint Identifiers (TEIDs) are used to identify GTP sessions.

dp-keep-assist-sessions {disable | enable}

This option is visible on the CLI but cannot be changed.

dp-load-distribution-method {to-master | round-robin | src-ip | dst-ip | src-dst-ip | src-ip-sport | dst-ip-dport | src-dst-ip-sport-dport}

Set the method used to load balance sessions among FPCs. Usually you would only need to change the load balancing method if you had specific requirements or you found that the default method wasn't distributing sessions in the manner that you would prefer. The default is `src-dst-ip-sport-dport` which means sessions are identified by their source address and port and destination address and port.

`to-master` directs all session to the primary FPC. This method is for troubleshooting only and should not be used for normal operation. Directing all sessions to the primary FPC will have a negative impact on performance.

`src-ip` sessions are distributed across all FPCs according to their source IP address.

`dst-ip` sessions are statically distributed across all FPCs according to their destination IP address.

`src-dst-ip` sessions are distributed across all FPCs according to their source and destination IP addresses.

`src-ip-sport` sessions are distributed across all FPCs according to their source IP address and source port.

`dst-ip-dport` sessions are distributed across all FPCs according to their destination IP address and destination port.

`src-dst-ipsport-dport` distribute sessions across all FPCs according to their source and destination IP address, source port, and destination port. This is the default load balance algorithm and represents true session-aware load

balancing. Session aware load balancing takes all session information into account when deciding where to send new sessions and where to send additional packets that are part of an already established session.

The `src-ip` and `dst-ip` load balancing methods use layer 3 information (IP addresses) to identify and load balance sessions. All of the other load balancing methods (except for `to-master`) use both layer 3 and layer 4 information (IP addresses and port numbers) to identify a TCP and UDP session. The layer 3 and layer 4 load balancing methods only use layer 3 information for other types of traffic (SCTP, ICMP, and ESP). If GTP load balancing is enabled, Tunnel Endpoint Identifiers (TEIDs) are used to identify GTP sessions.

dp-icmp-distribution-method {to-master | src-ip | dst-ip | src-dst-ip | derived}

Set the method used to load balance ICMP sessions among FPCs. Usually you would only need to change the load balancing method if you had specific requirements or you found that the default method wasn't distributing sessions in the manner that you would prefer. The default is `to-master`, which means all ICMP sessions are sent to the primary (master) FPC.

`to-master` directs all ICMP session to the primary FPC.

`src-ip` ICMP sessions are distributed across all FPCs according to their source IP address.

`dst-ip` ICMP sessions are statically distributed across all FPCs according to their destination IP address.

`src-dst-ip` ICMP sessions are distributed across all FPCs according to their source and destination IP addresses.

`derived` ICMP sessions are load balanced using the `dp-load-distribution-method` setting. Since port-based ICMP load balancing is not possible, if `dp-load-distribution-method` is set to a load balancing method that includes ports, ICMP load balancing will use the equivalent load balancing method that does not include ports. For example, if `dp-load-distribution-method` is set to the `src-dst-ip-sport-dport` (the default) then ICMP load balancing will use `src-dst-ip` load balancing.

dp-session-table-type {vdom-based | intf-vlan-based}

`dp-session-table-type` will be supported in a future version. For FortiOS 6.0.4, `dp-session-table-type` must be set to `intf-vlan-based` (the default value).

config workers

Set the weight and enable or disable each worker (FPC). Use the edit command to specify the slot the FPC is installed in. You can enable or disable each FPC and set a weight for each FPC.

The weight range is 1 to 10. 5 is average (and the default), 1 is -80% of average and 10 is +100% of average. The weights take effect if `weighted-loadbalance` is enabled.

```
config workers
   edit 3
      set status enable
      set weight 5
   end
```

config system console-server

Use this command to disable or enable the FortiGate-6000 console server. The console server allows you to use the `execute system console server` command from the management board CLI to access individual FPC consoles in your FortiGate-6000.

Syntax

```
config system console-server
   set status {disable | enable}
      config entries
         edit <slot>
      end
```

set status {disable | enable}

Disable or enable the FortiGate-6000 console server. Enabled by default.

FortiGate-6000 execute CLI commands

This chapter describes the FortiGate-6000 execute commands. Many of these commands are only available from the management board CLI.

execute load-balance load-backup-image <slot>

After uploading a firmware image onto the FortiGate-6000 internal TFTP server, use this command to install this firmware image onto an FPC as the backup firmware image. `<slot>` is the FPC slot number.

See Installing firmware on an individual FPC on page 19 for information about how to transfer a firmware image to the internal TFTP server.

execute load-balance slot manage [<chassis>.]<slot>

Log into the CLI of an individual FPC. Use `<slot>` to specify the FPC slot number. Use `<chassis>` to specify the chassis number in an HA configuration.

You will be asked to authenticate to connect to the FIM or FPM. Use the `exit` command to end the session and return to the CLI from which you ran the execute command.

execute load-balance slot nmi-reset <slot-map>

Perform an NMI reset on selected FPCs. The NMI reset dumps registers and backtraces of one or more FPCs to the console. After the data is dumped, the FPCs reboot. While the FPCs are rebooting, traffic is distributed to the remaining FPCs. The FPCs should restart normally and traffic can resume once they are up and running. You can use the `diagnose sys confsync status` command to verify that the FPCs have started up.

`<slot-map>` can be one or more FPC slot numbers or slot number ranges with no space and separated by commas. For example, to perform an NMI reset of slots 1, 3, 4, and 5, enter

```
execute load-balance slot nmi-reset 1,3-5
```

execute load-balance slot power-off <slot-map>

Power off selected FPCs. This command shuts down the FPC immediately. You can use the `diagnose sys confsync status` command to verify that the management board cannot communicate with the FPCs.

You can use the `execute load-balance slot power-on` command to start up powered off FPCs.

execute load-balance slot power-on <slot-map>

Power on and start up selected FPCs. It may take a few minutes for the FPCs to start up. You can use the `diagnose sys confsync status` command to verify that the FPCs have started up.

execute load-balance slot reboot <slot-map>

Restart selected FPCs. It may take a few minutes for the FPCs to shut down and restart. You can use the `diagnose sys confsync status` command to verify that the FPCs have started up.

execute load-balance update image <slot>

After uploading a firmware image onto the FortiGate-6000 internal TFTP server, use this command to install this firmware image onto an FPC. `<slot>` is the FPC slot number. The firmware image is installed and the FPC restarts running the new firmware.

For more information, see Installing firmware on an individual FPC on page 19.

execute system console-server

From the management board CLI, the `execute system console server` command provides access to individual FPC consoles in your FortiGate-6000. Console access can be useful for troubleshooting. For example, if an FPC does not boot properly you can use console access to view the state of the FPC and enter commands to fix the problem or restart the FPC.

The `execute system console-server` commands allow access only to FPCs in the FortiGate-6000 that you are logged into. You can't use this command to access FPCs in the other FortiGate-6000 in an HA configuration.

You can use the `config system console-server` command to enable or disable the console server (enabled by default). For more information, see config system console-server on page 78.

execute system console-server clearline <line>

Clear an active console server. You can use this command to stop a console-server session that you have started with the `execute system console-server connect` command. `<line>` is the console server session number. Use the `execute system console-server showline` command to view the active console server sessions.

execute system console-server connect <slot>

Start a console-server connection from the management board CLI to an FPC CLI. `<slot>` is the FPC slot number. Authenticate to log into the console and use CLI commands to view information, make changes, or restart the FPC. When you are done, use **Ctrl-X** to exit from the console back to the management board CLI.

Using **Ctrl-X** may not work if you are accessing the CLI console from the GUI. Instead you may need to log out of the GUI and then log back in.

execute system console-server showline

Show active console-server sessions.

execute upload image {ftp | tftp | usb}

Use this command to upload a firmware image to the FortiGate-6000 internal TFTP server. Once you have uploaded this firmware image, you can install it on an FPC using the `execute load-balance load-backup-image <slot>` command.

You can get the firmware image from an external FTP server, an external TFTP server, or from a USB key plugged in the FortiGate-6000 USB port. Use the following syntax:

```
execute upload image ftp <image-file-and-path> <comment> <ftp-server-address> <username>
     <password>
execute upload image tftp <image-file> <comment> <tftp-server-address>
execute upload image usb <image-file-and-path> <comment>
```