FortiGate-7000 - 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-7000 6.0.4 Handbook
01-604-396655-20191206

TABLE OF CONTENTS

Change log

Date	Change description
December 6, 2019	Corrections to FortiGate-7000 IPsec VPN on page 66 and FortiGate-7000 IPsec VPN load balancing on page 66. New sections: ICAP support on page 100 and SSL mirroring support on page 102.
July 10, 2019	New section: Adding a flow rule to support DHCP relay on page 57. Formerly missing commands added to FortiGate-7000 execute CLI commands on page 116. Additional changes and fixes throughout the document.
June 20, 2019	New section: Default Security Fabric configuration on page 104.
April 30, 2019	Fixes and updates throughout the document.
April 29, 2019	Minor updates.
April 26, 2019	Fixes and updates throughout the document.
April 26, 2019	FortiOS 6.0.4 document release.

What's new for FortiGate-7000 v6.0.4

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 FPM and FIM activity on page 51.
- New diagnose command to show how the DP processor will load balance a session, see Showing how the DP2 processor will load balance a session on page 52.
- Enabling or disabling synchronizing connectionless sessions, see Enabling session synchronization for TCP, SCTP, and connectionless sessions on page 85.
- ICMP traffic can now be load balanced, see ICMP load balancing on page 57.
- FortiGate Session Life Support Protocol (FGSP) support, see FortiGate-7000 FGSP HA on page 95.

FortiGate-7000 overview

A FortiGate-7000 product consists of a FortiGate-7000 series chassis (for example, the FortiGate-7040E) with FortiGate-7000 modules installed in the chassis slots. A FortiGate-7040E chassis comes with two interface modules (FIM) to be installed in slots 1 and 2 to provide network connections and session-aware load balancing to two processor modules (FPM) to be installed in slots 3 and 4.

FortiGate-7000 products are sold and licensed as packages that include the chassis as well as the modules to be included in the chassis. When you receive your FortiGate-7000 series product the chassis has to be installed in a rack and the modules installed in the chassis. Interface modules always go in slots 1 and 2 and processor modules in slots 3 and up.

If your FortiGate-7000 product includes two different interfaces modules, for optimal configuration you should install the module with the lower model number in slot 1 and the module with the higher model number in slot 2. For example, if your chassis includes a FIM-7901E and a FIM-7904E, install the FIM-7901E in chassis slot 1 and the FIM-7904E in chassis slot 2. This applies to any combination of two different interface modules.

As an administrator, when you browse to the FortiGate-7000 management IP address you log into the interface module in slot 1 (the primary or master interface module or FIM) to view the status of the FortiGate-7000 and make configuration changes. The FortiOS firmware running on each module has the same configuration and when you make configuration changes to the primary interface module, the configuration changes are synchronized to all modules.

The same FortiOS firmware build runs on each module in the chassis. You can upgrade FortiGate-7000 firmware by logging into the primary interface module and performing a firmware upgrade as you would for any FortiGate. During the upgrade process the firmware of all of the modules in the chassis upgrades in one step. Firmware upgrades should be done during a quiet time because traffic will briefly be interrupted during the upgrade process.

Licenses, device registration, and support

A FortiGate-7000 product is made up of a FortiGate-7000 series chassis, one or two FIM interface modules and two to four FPM processor modules. The entire package is licensed and configured as a single product under the FortiGate-7000 chassis serial number. When you receive a new FortiGate-7000 product you register it on https://support.fortinet.com using the chassis serial number. Use the chassis serial number when requesting support from Fortinet for the product.

All Fortinet licensing, including FortiCare Support, IPS, AntiVirus, Web Filtering, Mobile Malware, FortiClient, FortiCloud, and additional virtual domains (VDOM) is for the entire FortiGate-7000 product and not for individual components.

If an individual component, such as a single interface or processor fails you can RMA and replace just that component.

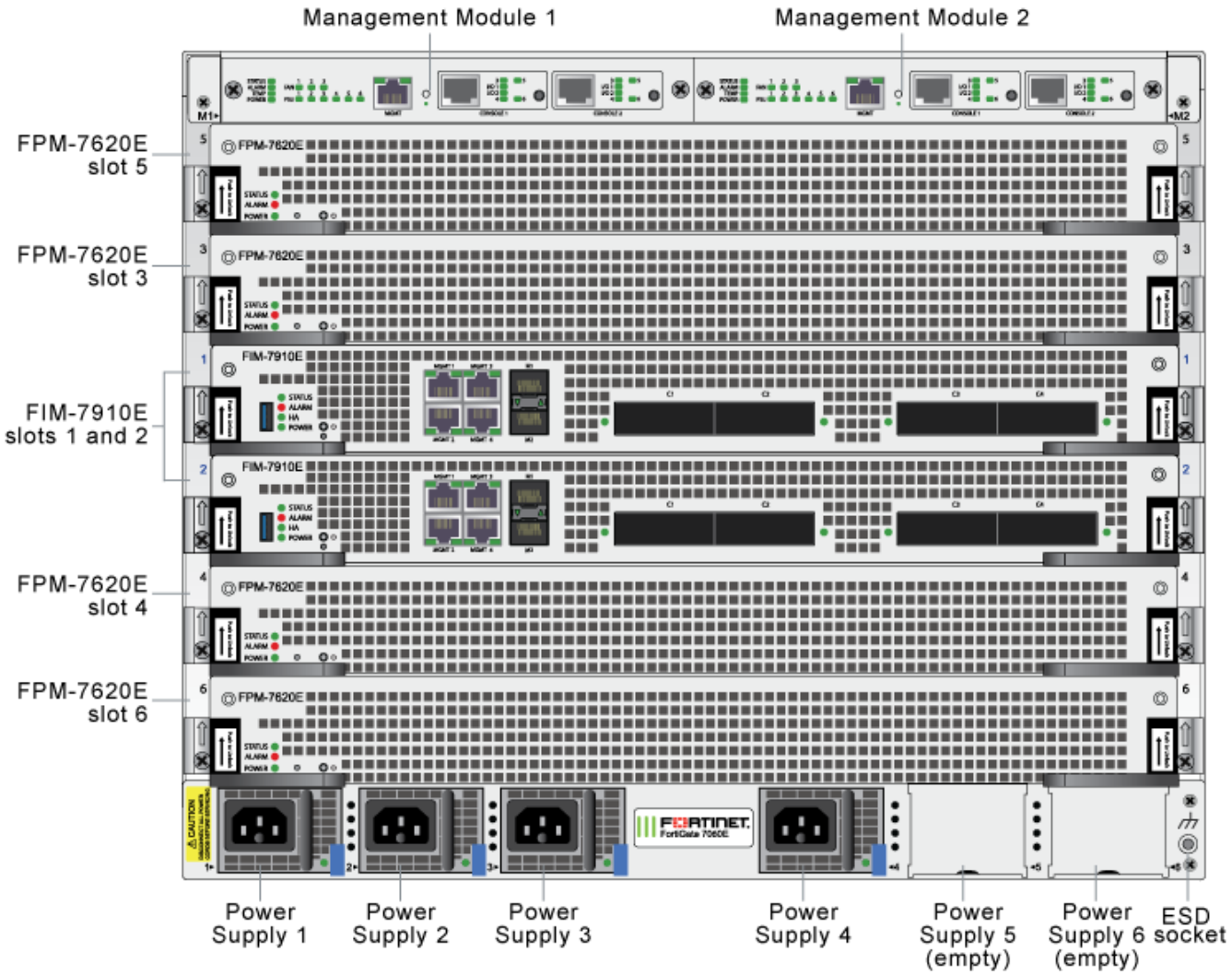
FortiGate-7060E

The FortiGate-7060E is a 8U 19-inch rackmount 6-slot chassis with a 80Gbps fabric and 1Gbps base backplane designed by Fortinet. The fabric backplane provides network data communication and the base backplane provides management and synch communication among the chassis slots.

FortiGate-7060E front panel

The chassis is managed by two redundant management modules. Each module includes an Ethernet connection as well as two switchable console ports that provide console connections to the modules in the chassis slots. The active management module controls chassis cooling and power management and provides an interface for managing the modules installed in the chassis.

FortiGate-7060E front panel, (example module configuration)

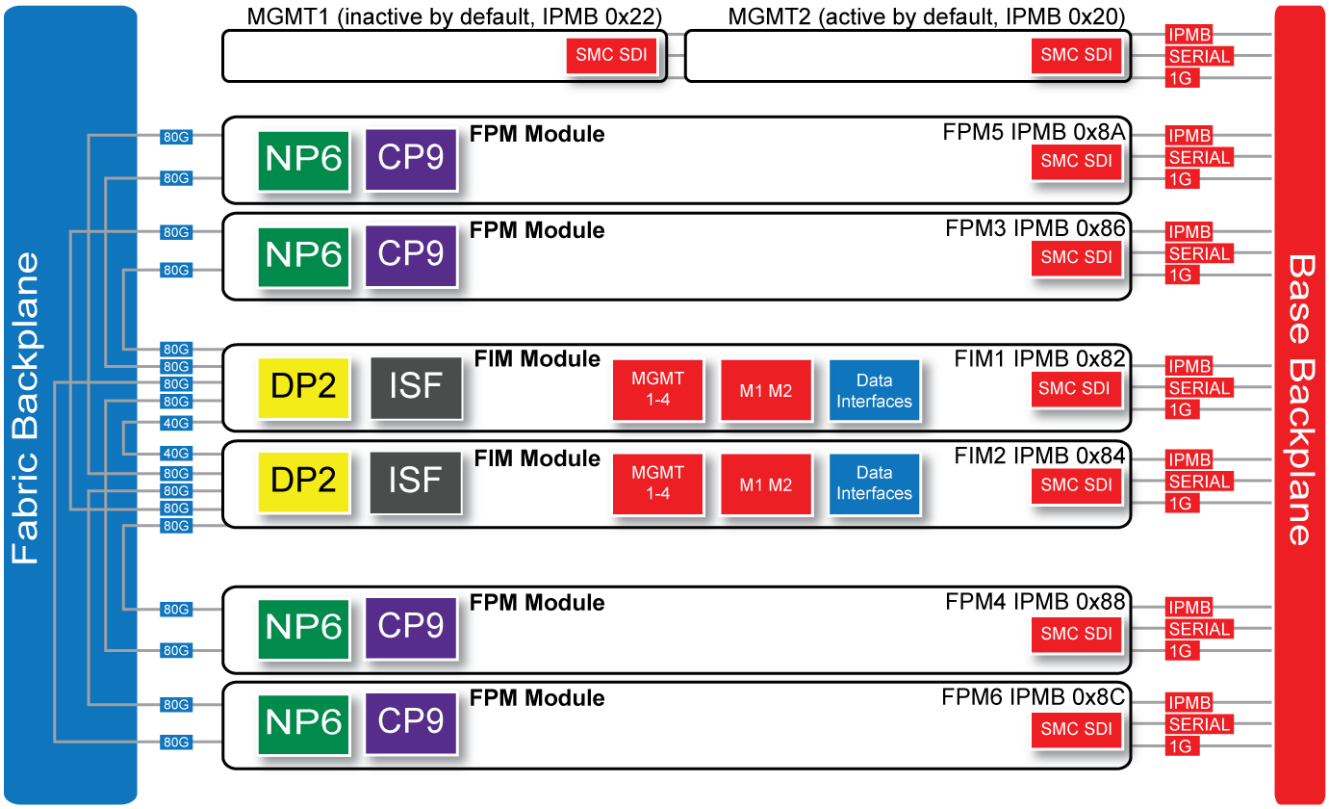


Power is provided to the chassis using four hot swappable 3+1 redundant 100-240 VAC, 50-60 Hz power supply units (PSUs). You can also optionally add up to six PSUs to provide 3+3 redundancy. The FortiGate-7060E can also be equipped with DC PSUs allowing you to connect the chassis to -48V DC power

The standard configuration of the FortiGate-7060E includes two FIM (interface) modules in chassis slots 1 and 2 and up to four FPM (processing) modules in chassis slots 3 to 6.

FortiGate-7060E schematic

The FortiGate-7060E chassis schematic below shows the communication channels between chassis components including the management modules (MGMT), the FIMs (called FIM1 and FIM2) and the FPMs (FPM3, FPM4, FPM5, and FPM6).



By default, MGMT2 is the active management module and MGMT1 is inactive. The active management module always has the Intelligent Platform Management Bus (IPMB) address 0x20 and the inactive management module always has the IPMB address 0x22.

The active management module communicates with all modules in the chassis over the base backplane. Each module, including the management modules has a Shelf Management Controller (SMC). These SMCs support IPMB communication between the active management module and the FIM and FPMs for storing and sharing sensor data that the management module uses to control chassis cooling and power distribution. The base backplane also supports serial communications to allow console access from the management module to all modules, and 1Gbps Ethernet communication for management and heartbeat communication between modules.

FIM1 and FIM2 (IPMB addresses 0x82 and 0x84) are the FIMs in slots 1 and 2. The interfaces of these modules connect the chassis to data networks and can be used for Ethernet management access to chassis components. The FIMs include DP2 processors that distribute sessions over the Integrated Switch Fabric (ISF) to the NP6 processors in the FPMs. Data sessions are communicated to the FPMs over the 80Gbps chassis fabric backplane.

FPM03, FPM04, FPM05, and FPM06 (IPMB addresses 0x86, 0x88, 0x8A, and 0x8C) are the FPM processor modules in slots 3 to 6. These worker modules process sessions distributed to them by the FIMs. FPMs include NP6 processors to offload sessions from the FPM CPU and CP9 processors that accelerate content processing.

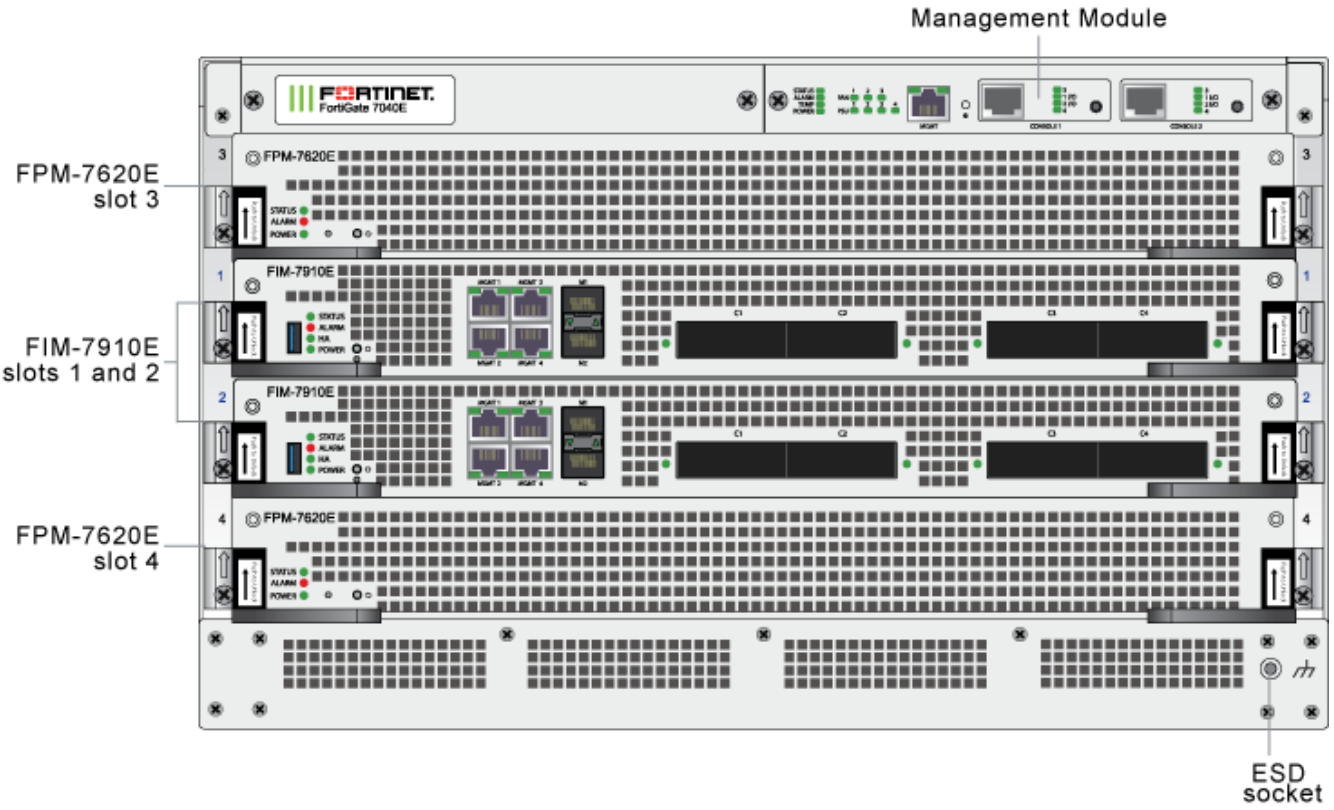
FortiGate-7040E

The FortiGate-7040E is a 6U 19-inch rackmount 4-slot chassis with a 80Gbps fabric and 1Gbps base backplane designed by Fortinet. The fabric backplane provides network data communication and the base backplane provides management and synch communication among the chassis slots.

FortiGate-7040E front panel

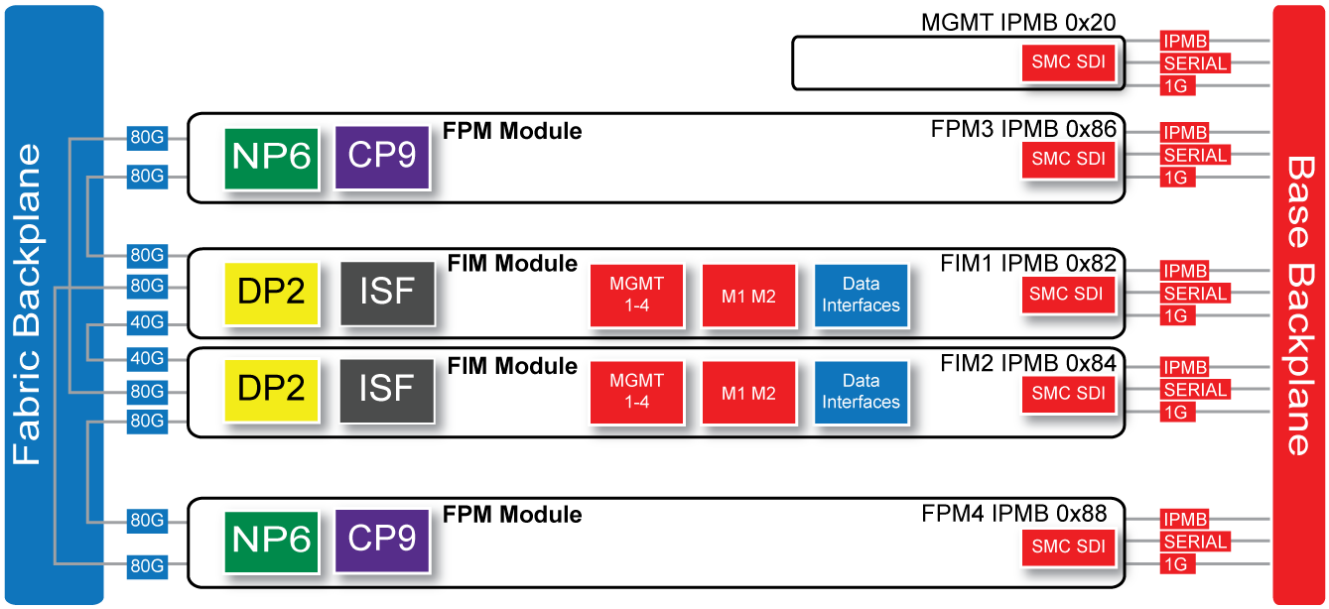
The FortiGate-7040E chassis is managed by a single management module that includes an Ethernet connection as well as two switchable console ports that provide console connections to the modules in the chassis slots. The management module controls chassis cooling and power management and provides an interface for managing the modules installed in the chassis. The standard configuration of the FortiGate-7040E includes two FIM (interface) modules in chassis slots 1 and 2 and two FPM (processing) modules in chassis slots 3 and 4.

FortiGate-7040E front panel



FortiGate-7040E schematic

The FortiGate-7040E chassis schematic below shows the communication channels between chassis components including the management module (MGMT), the FIMs (called FIM1 and FIM2) and the FPMs (FPM3 and FPM4).



The management module (MGMT, with Intelligent Platform Management Bus (IPMB) address 0x20) communicates with all modules in the chassis over the base backplane. Each module, including the management module, includes a Shelf Management Controller (SMC). These SMCs support IPMB communication between the management module and the FIM and FPMs for storing and sharing sensor data that the management module uses to control chassis cooling and power distribution. The base backplane also supports serial communications to allow console access from the management module to all modules, and 1Gbps Ethernet communication for management and heartbeat communication between modules.

FIM1 and FIM2 (IPMB addresses 0x82 and 0x84) are the FIMs in slots 1 and 2. The interfaces of these modules connect the chassis to data networks and can be used for Ethernet management access to chassis components. The FIMs include DP2 processors that distribute sessions over the Integrated Switch Fabric (ISF) to the NP6 processors in the FPMs. Data sessions are communicated to the FPMs over the 80Gbps chassis fabric backplane.

FPM3 and FPM4 (IPMB addresses 0x86 and 0x88) are the FPM processor modules in slots 3 and 4. These worker modules process sessions distributed to them by the FIMs. FPMs include NP6 processors to offload sessions from the FPM CPU and CP9 processors that accelerate content processing.

FortiGate-7030E

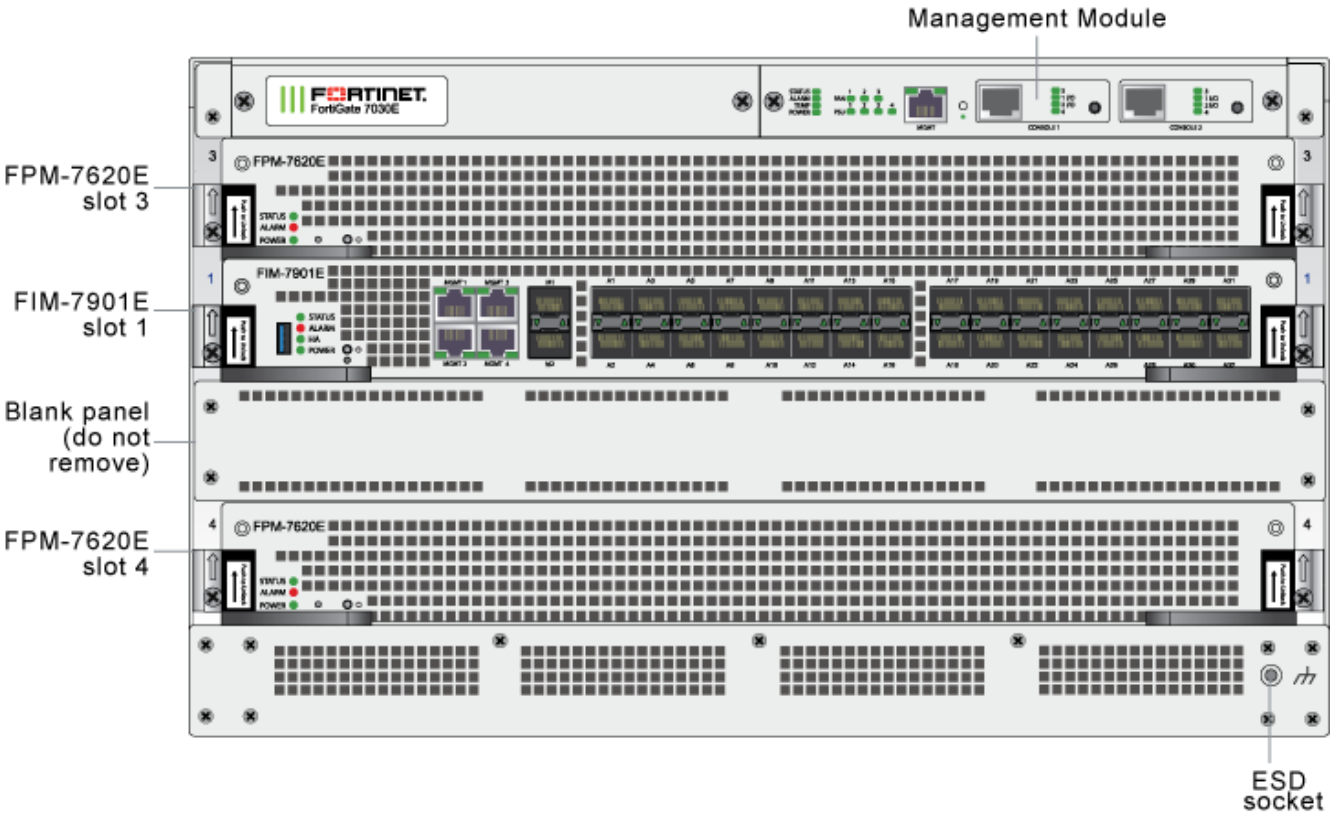
The FortiGate-7030E is a 6U 19-inch rackmount 3-slot chassis with a 80Gbps fabric and 1Gbps base backplane designed by Fortinet. The fabric backplane provides network data communication and the base backplane provides management and synch communication among the chassis slots.

FortiGate-7030E front panel

The FortiGate-7030E chassis is managed by a single management module that includes an Ethernet connection as well as two switchable console ports that provide console connections to the modules in the chassis slots. The management module controls chassis cooling and power management and provides an interface for managing the modules installed in the chassis. The standard configuration of the FortiGate-7030E includes one FIM (interface) module in chassis slot 1

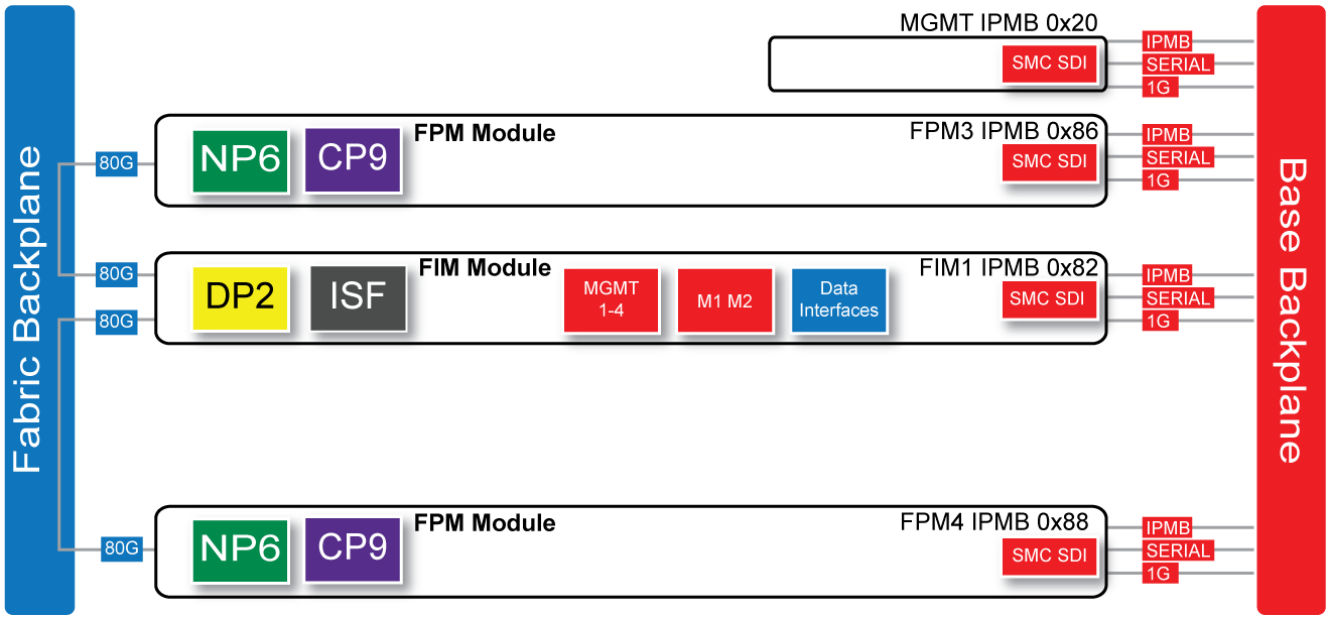
and two FPM (processing) modules in chassis slots 3 and 4. The front panel also includes a sealed blank panel. Breaking the seal or removing the panel voids your FortiGate-7030E warranty.

FortiGate-7030E front panel (example module configuration)



FortiGate-7030E schematic

The FortiGate-7030E chassis schematic below shows the communication channels between chassis components including the management module (MGMT), the FIM (called FIM1) and the FPMs (FPM3 and FPM4).



The management module (MGMT, with Intelligent Platform Management Bus (IPMB) address 0x20) communicates with all modules in the chassis over the base backplane. Each module, including the management module includes a Shelf Management Controller (SMC). These SMCs support IPMB communication between the management module and the FIM and FPMs for storing and sharing sensor data that the management module uses to control chassis cooling and power distribution. The base backplane also supports serial communications to allow console access from the management module to all modules, and 1Gbps Ethernet communication for management and heartbeat communication between modules.

FIM1 (IPMB address 0x82) is the FIM in slot 1. The interfaces of this module connect the chassis to data networks and can be used for Ethernet management access to chassis components. The FIM includes DP2 processors that distribute sessions over the Integrated Switch Fabric (ISF) to the NP6 processors in the FPMs. Data sessions are communicated to the FPMs over the 80Gbps chassis fabric backplane.

FPM3 and FPM4 (IPMB addresses 0x86 and 0x88) are the FPM processor modules in slots 3 and 4. These worker modules process sessions distributed to them by the FIM. FPMs include NP6 processors to offload sessions from the FPM CPU and CP9 processors that accelerate content processing.

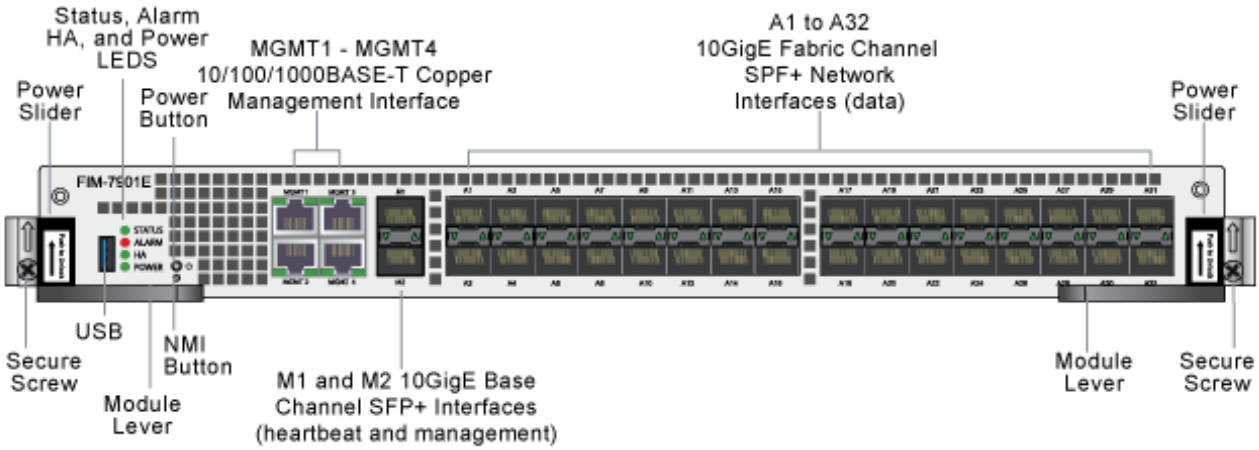
FIM-7901E interface module

The FIM-7901E interface module is a hot swappable module that provides data, management and session sync/heartbeat interfaces, base backplane switching and fabric backplane session-aware load balancing for a FortiGate-7000 chassis. The FIM-7901E includes an integrated switch fabric and DP2 processors to load balance millions of data sessions over the chassis fabric backplane to FPM processor modules.

The FIM-7901E can be installed in any FortiGate-7000 series chassis in hub/switch slots 1 and 2. The FIM-7901E provides thirty-two 10GigE small form-factor pluggable plus (SPF+) interfaces for a FortiGate-7000 chassis.

You can also install FIM-7901Es in a second chassis and operate the chassis in HA mode with another set of processor modules to provide chassis failover protection.

FIM-7901E front panel



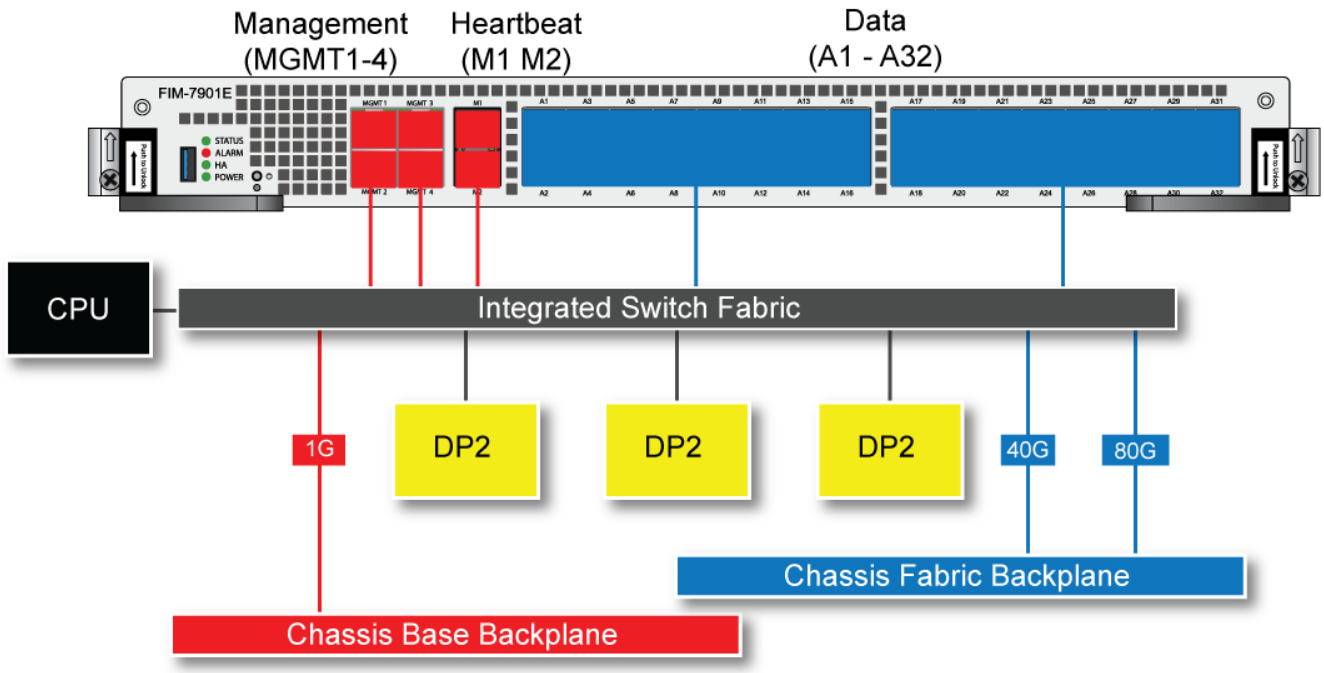
The FIM-7901E includes the following hardware features:

- Thirty-two front panel 10GigE SFP+ fabric channel interfaces (A1 to A32). These interfaces are connected to 10Gbps networks to distribute sessions to the FPM processor modules installed in chassis slots 3 and up. These interfaces can also be configured to operate as Gigabit Ethernet interfaces using SFP transceivers. These interfaces also support creating link aggregation groups (LAGs) that can include interfaces from both FIM-7901Es.
- Two front panel 10GigE SFP+ interfaces (M1 and M2) that connect to the base backplane channel. These interfaces are used for heartbeat, session sync, and management communication between FIM-7901Es in different chassis. These interfaces can also be configured to operate as Gigabit Ethernet interfaces using SFP transceivers, but should not normally be changed. If you use switches to connect these interfaces, the switch ports should be able to accept packets with a maximum frame size of at least 1526. The M1 and M2 interfaces need to be on different broadcast domains. If M1 and M2 are connected to the same switch, Q-in-Q must be enabled on the switch.
- Four 10/100/1000BASE-T out of band management Ethernet interfaces (MGMT1 to MGMT4).
- One 80Gbps fabric backplane channel for traffic distribution with each FPM installed in the same chassis as the FIM-7901E.
- One 1Gbps base backplane channel for base backplane with each FPM installed in the same chassis as the FIM-7901E.
- One 40Gbps fabric backplane channel for fabric backplane communication with the other FIM-7901E in the chassis.
- One 1Gbps base backplane channel for base backplane communication with the other FIM-7901E in the chassis.
- On-board DP2 processors and an integrated switch fabric to provide high-capacity session-aware load balancing.
- One front panel USB port.
- Power button.
- NMI switch (for troubleshooting as recommended by Fortinet Support).
- Mounting hardware.
- LED status indicators.

FIM-7901E schematic

The FIM-7901E includes an integrated switch fabric (ISF) that connects the FIM front panel interfaces to the DP2 session-aware load balancers and to the chassis fabric and base backplanes. The ISF also allows the DP2 processors to distribute sessions among all NP6 processors on the FortiGate Processor Modules (FPM) in the FortiGate-7000 chassis.

FIM-7901E schematic



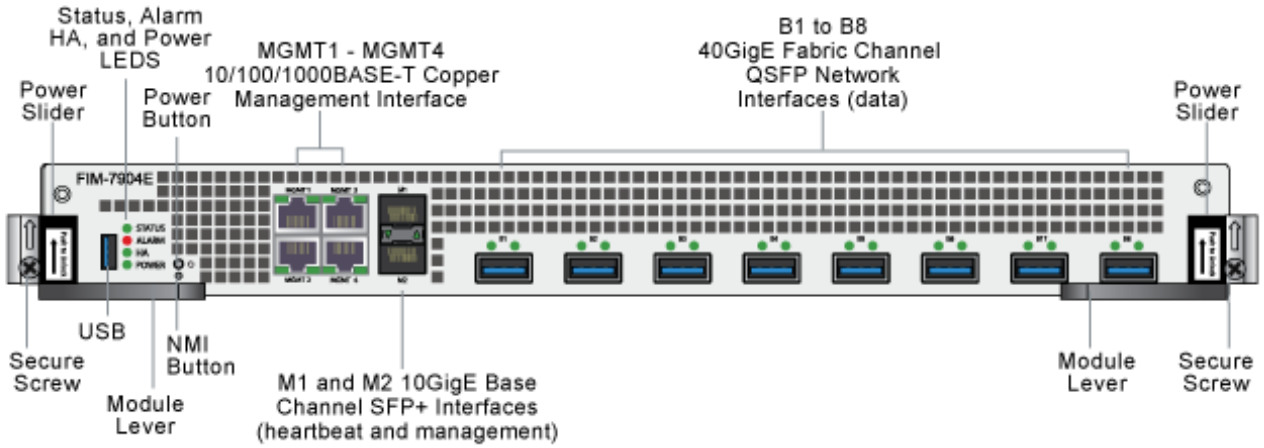
FIM-7904E interface module

The FIM-7904E interface module is a hot swappable module that provides data, management and session sync/heartbeat interfaces, base backplane switching and fabric backplane session-aware load balancing for a FortiGate-7000 series chassis. The FIM-7904E includes an integrated switch fabric and DP2 processors to load balance millions of data sessions over the chassis fabric backplane to FPM processor modules.

The FIM-7904E can be installed in any FortiGate-7000 series chassis in hub/switch slots 1 and 2. The FIM-7904E provides four Quad Small Form-factor Pluggable plus (QSFP+) interfaces for a FortiGate-7000 chassis. Using a 40GBASE-SR10 multimode QSFP+ transceiver, each QSFP+ interface can also be split into four 10GBASE-SR interfaces.

You can also install FIM-7904Es in a second chassis and operate the chassis in HA mode with another set of processor modules to provide chassis failover protection.

FIM-7904E front panel



The FIM-7904E includes the following hardware features:

- Eight front panel 40GigE QSFP+ fabric channel interfaces (B1 to B8). These interfaces are connected to 40Gbps networks to distribute sessions to the FPM processor modules installed in chassis slots 3 and up. Using 40GBASE-SR10 multimode QSFP+ transceivers, each QSFP+ interface can also be split into four 10GBASE-SR interfaces. These interfaces also support creating link aggregation groups (LAGs) that can include interfaces from both FIM-7904Es.
- Two front panel 10GigE SFP+ interfaces (M1 and M2) that connect to the base backplane channel. These interfaces are used for heartbeat, session sync, and management communication between FIM-7904Es in different chassis. These interfaces can also be configured to operate as Gigabit Ethernet interfaces using SFP transceivers, but should not normally be changed. If you use switches to connect these interfaces, the switch ports should be able to accept packets with a maximum frame size of at least 1526. The M1 and M2 interfaces need to be on different broadcast domains. If M1 and M2 are connected to the same switch, Q-in-Q must be enabled on the switch.
- Four 10/100/10000BASE-T out of band management Ethernet interfaces (MGMT1 to MGMT4).
- One 80Gbps fabric backplane channel for traffic distribution with each FPM installed in the same chassis as the FIM-7904E.
- One 1Gbps base backplane channel for base backplane with each FPM installed in the same chassis as the FIM-7904E.
- One 40Gbps fabric backplane channel for fabric backplane communication with the other FIM-7904E in the chassis.
- One 1Gbps base backplane channel for base backplane communication with the other FIM-7904E in the chassis.
- On-board DP2 processors and an integrated switch fabric to provide high-capacity session-aware load balancing.
- One front panel USB port.
- Power button.
- NMI switch (for troubleshooting as recommended by Fortinet Support).
- Mounting hardware.
- LED status indicators.

Splitting the FIM-7904E B1 to B8 interfaces

Each 40GE interface (B1 to B8) on the FIM-7904Es in slot 1 and slot 2 of a FortiGate-7000 system can be split into 4x10GBE interfaces. You split these interfaces after the FIM-7904Es are installed in your FortiGate-7000 system and the system us up and running. You can split the interfaces of the FIM-7904Es in slot 1 and slot 2 at the same time by entering a single CLI command. Splitting the interfaces requires a system reboot so Fortinet recommends that you split multiple interfaces at the same time according to your requirements to avoid traffic disruption.

For example, to split the B1 interface of the FIM-7904E in slot 1 (this interface is named 1-B1) and the B1 and B4 interfaces of the FIM-7904E in slot 2 (these interfaces are named 2-B1 and 2-B4) connect to the CLI of your FortiGate-7000 system using the management IP and enter the following command:

```
config system global
   set split-port 1-B1 2-B1 2-B4
end
```

After you enter the command, the FortiGate-7000 reboots and when it comes up:

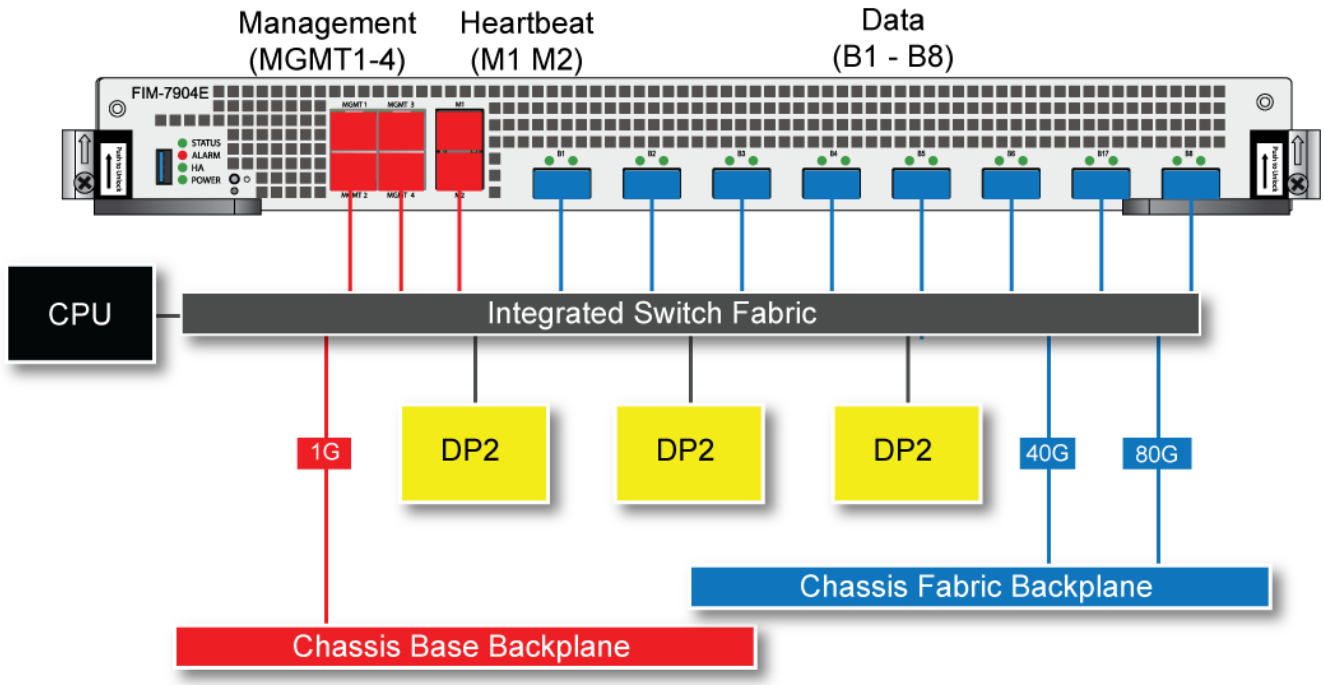
- The 1-B1 interface will no longer be available. Instead the 1-B1/1, 1-B1/2, 1-B1/3, and 1-B1/4 interfaces will be available.
- The 2-B1 interface will no longer be available. Instead the 2-B1/1, 2-B1/2, 2-B1/3, and 2-B1/4 interfaces will be available.
- The 2-B4 interface will no longer be available. Instead the 2-B4/1, 2-B4/2, 2-B4/3, and 2-B4/4 interfaces will be available.

You can now connect breakout cables to these interfaces and configure traffic between them just like any other FortiGate interface.

FIM-7904E hardware schematic

The FIM-7904E includes an integrated switch fabric (ISF) that connects the front panel interfaces to the DP2 session-aware load balancers and to the chassis backplanes. The ISF also allows the DP2 processors to distribute sessions among all NP6 processors on the FortiGate Processor Modules (FPM) in the FortiGate-7000 chassis.

FIM-7904E hardware architecture

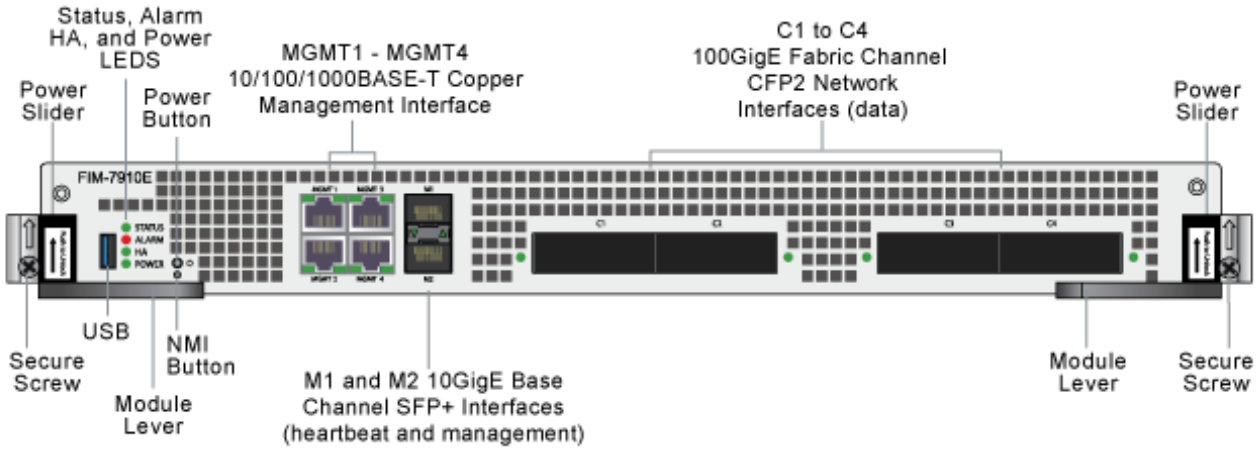


FIM-7910E interface module

The FIM-7910E interface module is a hot swappable module that provides data, management and session sync/heartbeat interfaces, base backplane switching and fabric backplane session-aware load balancing for a FortiGate-7000 series chassis. The FIM-7910E includes an integrated switch fabric and DP2 processors to load balance millions of data sessions over the chassis fabric backplane to FPM processor modules.

The FIM-7910E can be installed in any FortiGate-7000 series chassis in hub/switch slots 1 and 2. The FIM-7910E provides four C form-factor pluggable 2 (CFP2) interfaces for a FortiGate-7000 chassis. Using a 100GBASE-SR10 multimode CFP2 transceiver, each CFP2 interface can also be split into ten 10GBASE-SR interfaces.

FIM-7910E front panel



The FIM-7910E includes the following hardware features:

- Four front panel 100GigE CFP2 fabric channel interfaces (C1 to C4). These interfaces are connected to 100Gbps networks to distribute sessions to the FPM processor modules installed in chassis slots 3 and up. Using 100GBASE-SR10 multimode CFP2 transceivers, each CFP2 interface can also be split into ten 10GBASE-SR interfaces. These interfaces also support creating link aggregation groups (LAGs) that can include interfaces from both FIM-7910Es.
- Two front panel 10GigE SFP+ interfaces (M1 and M2) that connect to the base backplane channel. These interfaces are used for heartbeat, session sync, and management communication between FIM-7910Es in different chassis. These interfaces can also be configured to operate as Gigabit Ethernet interfaces using SFP transceivers, but should not normally be changed. If you use switches to connect these interfaces, the switch ports should be able to accept packets with a maximum frame size of at least 1526. The M1 and M2 interfaces need to be on different broadcast domains. If M1 and M2 are connected to the same switch, Q-in-Q must be enabled on the switch.
- Four 10/100/1000BASE-T out of band management Ethernet interfaces (MGMT1 to MGMT4).
- One 80Gbps fabric backplane channel for traffic distribution with each FPM installed in the same chassis as the FIM-7910E.
- One 1Gbps base backplane channel for base backplane with each FPM installed in the same chassis as the FIM-7910E.
- One 40Gbps fabric backplane channel for fabric backplane communication with the other FIM-7910E in the chassis.
- One 1Gbps base backplane channel for base backplane communication with the other FIM-7910E in the chassis.
- On-board DP2 processors and an integrated switch fabric to provide high-capacity session-aware load balancing.
- One front panel USB port.
- Power button.
- NMI switch (for troubleshooting as recommended by Fortinet Support).
- Mounting hardware.
- LED status indicators.

Splitting the FIM-7910E C1 to C4 interfaces

Each 100GE interface (C1 to C4) on the FIM-7910Es in slot 1 and slot 2 of a FortiGate-7000 system can be split into 10 x 10GBE interfaces. You split these interfaces after the FIM-7910Es are installed in your FortiGate-7000 system and the system us up and running. You can split the interfaces of the FIM-7910Es in slot 1 and slot 2 at the same time by entering a single CLI command. Splitting the interfaces requires a system reboot so Fortinet recommends that you split multiple interfaces at the same time according to your requirements to avoid traffic disruption.

For example, to split the C1 interface of the FIM-7910E in slot 1 (this interface is named 1-C1) and the C1 and C4 interfaces of the FIM-7910E in slot 2 (these interfaces are named 2-C1 and 2-C4) connect to the CLI of your FortiGate-7000 system using the management IP and enter the following command:

```
config system global
   set split-port 1-C1 2-C1 2-C4
end
```

After you enter the command, the FortiGate-7000 reboots and when it comes up:

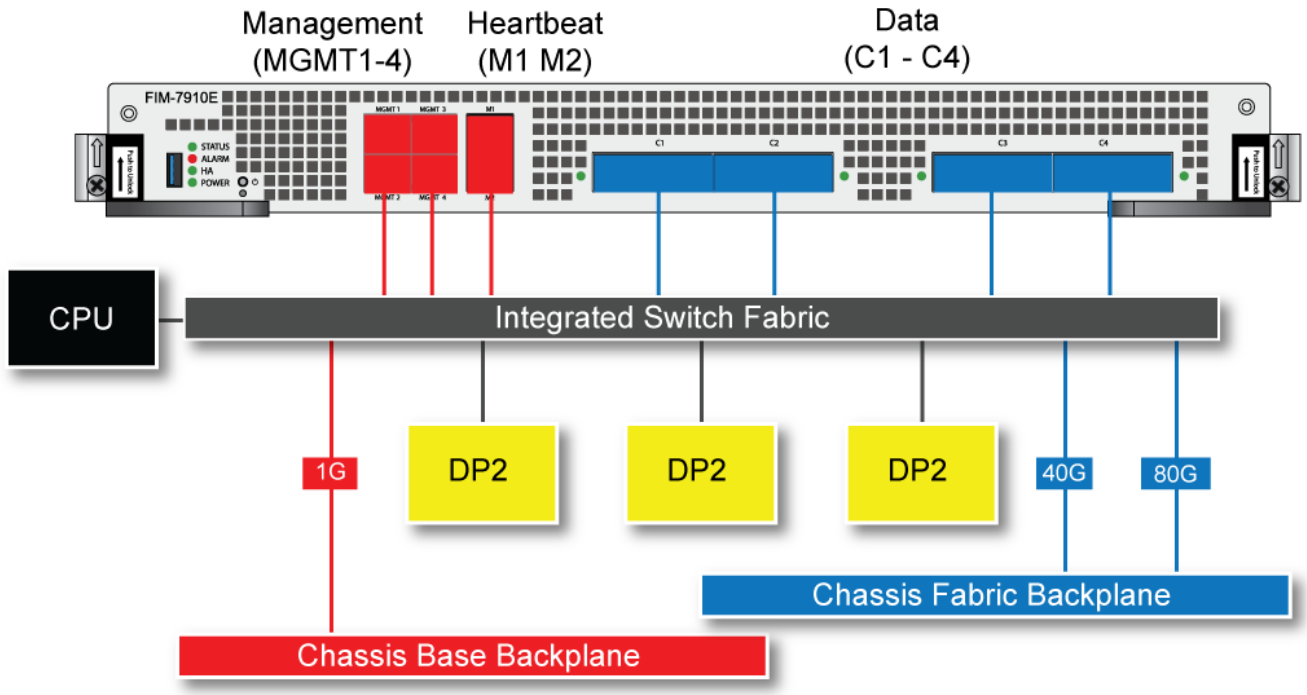
- The 1-C1 interface will no longer be available. Instead the 1-C1/1, 1-C1/2, ..., and 1-C1/10 interfaces will be available.
- The 2-C1 interface will no longer be available. Instead the 2-C1/1, 2-C1/2, ..., and 2-C1/10 interfaces will be available.
- The 2-C4 interface will no longer be available. Instead the 2-C4/1, 2-C4/2, ..., and 2-C4/10 interfaces will be available.

You can now connect breakout cables to these interfaces and configure traffic between them just like any other FortiGate interface.

FIM-7910E hardware schematic

The FIM-7910E includes an integrated switch fabric (ISF) that connects the front panel interfaces to the DP2 session-aware load balancers and to the chassis backplanes. The ISF also allows the DP2 processors to distribute sessions among all NP6 processors on the FortiGate Processor Modules (FPM) in the FortiGate-7000chassis.

FIM-7910E hardware schematic



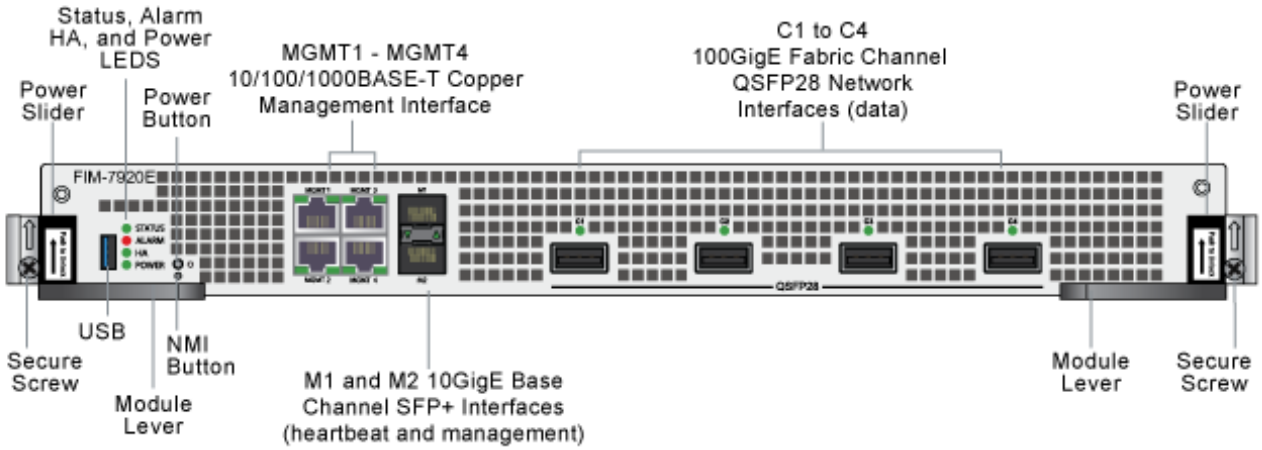
FIM-7920E interface module

The FIM-7920E interface module is a hot swappable module that provides data, management and session sync/heartbeat interfaces, base backplane switching and fabric backplane session-aware load balancing for a FortiGate-7000 series chassis. The FIM-7920E includes an integrated switch fabric and DP2 processors to load balance millions of data sessions over the chassis fabric backplane to FPM processor modules.

The FIM-7920E can be installed in any FortiGate-7000 series chassis in hub/switch slots 1 or 2. The FIM-7920E provides four Quad Small Form-factor Pluggable 28 (QSFP28) 100GigE interfaces for a FortiGate-7000 chassis. Using a 100GBASE-SR4 QSFP28 or 40GBASE-SR4 QSFP+ transceiver, each QSFP28 interface can also be split into four 10GBASE-SR interfaces.

You can also install FIM-7920Es in a second chassis and operate the chassis in HA mode with another set of processor modules to provide chassis failover protection.

FIM-7920E front panel



The FIM-7920E includes the following hardware features:

- Four front panel 100GigE QSFP28 fabric channel interfaces (C1 to C4). These interfaces are connected to 100Gbps networks to distribute sessions to the FPM processor modules installed in chassis slots 3 and up. Using a 100GBASE-SR4 QSFP28 or 40GBASE-SR4 QSFP+ transceiver, each QSFP28 interface can also be split into four 10GBASE-SR interfaces. These interfaces also support creating link aggregation groups (LAGs) that can include interfaces from both FIM-7920Es.
- Two front panel 10GigE SFP+ interfaces (M1 and M2) that connect to the base backplane channel. These interfaces are used for heartbeat, session sync, and management communication between FIM-7920Es in different chassis. These interfaces can also be configured to operate as Gigabit Ethernet interfaces using SFP transceivers, but should not normally be changed. If you use switches to connect these interfaces, the switch ports should be able to accept packets with a maximum frame size of at least 1526. The M1 and M2 interfaces need to be on different broadcast domains. If M1 and M2 are connected to the same switch, Q-in-Q must be enabled on the switch.
- Four 10/100/1000BASE-T out of band management Ethernet interfaces (MGMT1 to MGMT4).
- One 80Gbps fabric backplane channel for traffic distribution with each FPM installed in the same chassis as the FIM-7920E.
- One 1Gbps base backplane channel for base backplane with each FPM installed in the same chassis as the FIM-7920E.
- One 40Gbps fabric backplane channel for fabric backplane communication with the other FIM-7920E in the chassis.
- One 1Gbps base backplane channel for base backplane communication with the other FIM-7920E in the chassis.
- On-board DP2 processors and an integrated switch fabric to provide high-capacity session-aware load balancing.
- One front panel USB port.
- Power button.
- NMI switch (for troubleshooting as recommended by Fortinet Support).
- Mounting hardware.
- LED status indicators.

Changing the interface type and splitting the FIM-7920E C1 to C4 interfaces

By default, the FIM-7920E C1 to C4 interfaces are configured as 100GE QSFP28 interfaces. You can use the following command to convert them to 40GE QSFP+ interfaces. Once converted, you can use the other command below to split them into four 10GBASE-SR interfaces.

Changing the interface type

For example, to change the interface type of the C1 interface of the FIM-7920E in slot 1 to 40GE QSFP+ connect to the CLI of your FortiGate-7000 system using the management IP and enter the following command:

```
config system global
   set qsfp28-40g-port 1-C1
end
```

The FortiGate-7000 system reboots and when it starts up interface C1 of the FIM-7920E in slot 1 is operating as a 40GE QSFP+ interface .

To change the interface type of the C3 and C4 ports of the FIM-7920E in slot 2 to 40GE QSFP+ enter the following command:

```
config system global
   set qsfp28-40g-port 2-C3 2-C4
end
```

The FortiGate-7000 system reboots and when it starts up interfaces C3 and C4 of the FIM-7920E in slot 2 are operating as a 40GE QSFP+ interfaces.

Splitting the C1 to C4 interfaces

Each 40GE interface (C1 to C4) on the FIM-7920Es in slot 1 and slot 2 of a FortiGate-7000 system can be split into 4 x 10GBE interfaces. You split these interfaces after the FIM-7920Es are installed in your FortiGate-7000 system and the system us up and running. You can split the interfaces of the FIM-7920Es in slot 1 and slot 2 at the same time by entering a single CLI command. Splitting the interfaces requires a system reboot so Fortinet recommends that you split multiple interfaces at the same time according to your requirements to avoid traffic disruption.

For example, to split the C1 interface of the FIM-7920E in slot 1 (this interface is named 1-C1) and the C1 and C4 interfaces of the FIM-7920E in slot 2 (these interfaces are named 2-C1 and 2-C4) connect to the CLI of your FortiGate-7000 system using the management IP and enter the following command:

```
config system global
   set split-port 1-C1 2-C1 2-C4
end
```

After you enter the command, the FortiGate-7000 reboots and when it comes up:

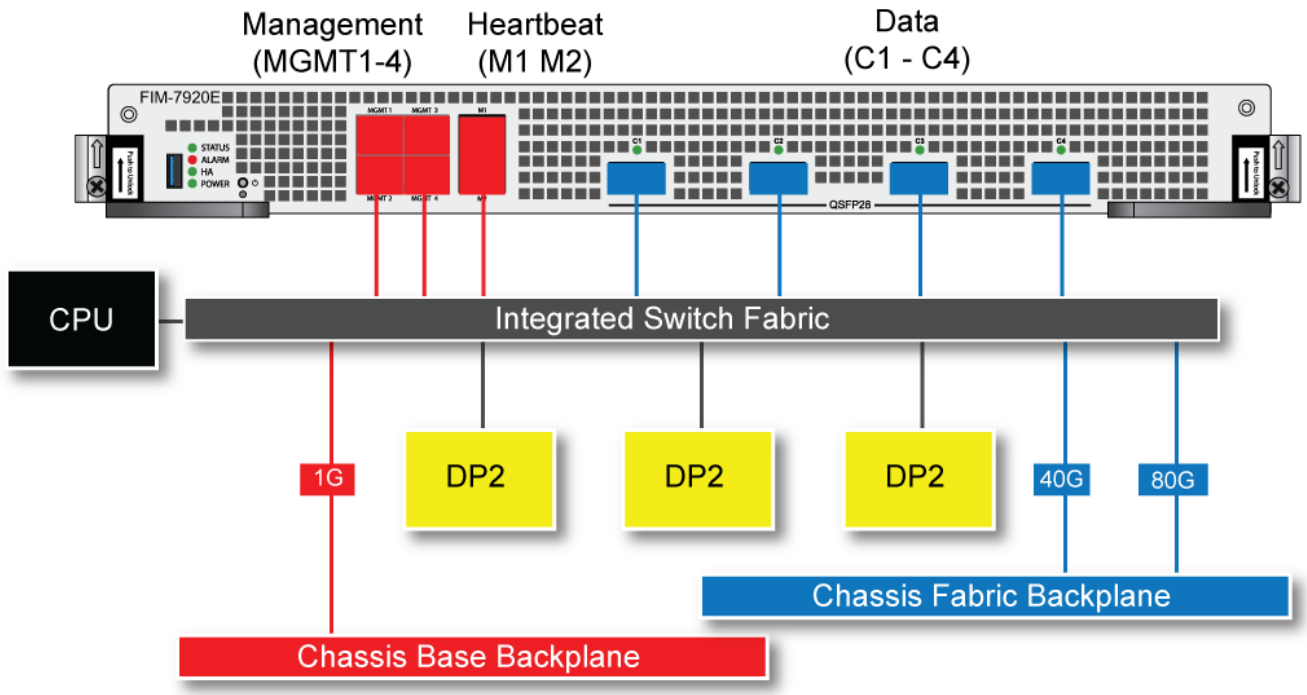
- The 1-C1 interface will no longer be available. Instead the 1-C1/1, 1-C1/2, 1-C1/3, and 1-C1/4 interfaces will be available.
- The 2-C1 interface will no longer be available. Instead the 2-C1/1, 2-C1/2, 2-C1/3, and 2-C1/4 interfaces will be available.
- The 2-C4 interface will no longer be available. Instead the 2-C4/1, 2-C4/2, 2-C4/3, and 2-C4/4 interfaces will be available.

You can now connect breakout cables to these interfaces and configure traffic between them just like any other FortiGate interface.

FIM-7920E hardware schematic

The FIM-7920E includes an integrated switch fabric (ISF) that connects the front panel interfaces to the DP2 session-aware load balancers and to the chassis backplanes. The ISF also allows the DP2 processors to distribute sessions among all NP6 processors on the FortiGate Processor Modules (FPM) in the FortiGate-7000 chassis.

FIM-7920E hardware schematic



FPM-7620E processing module

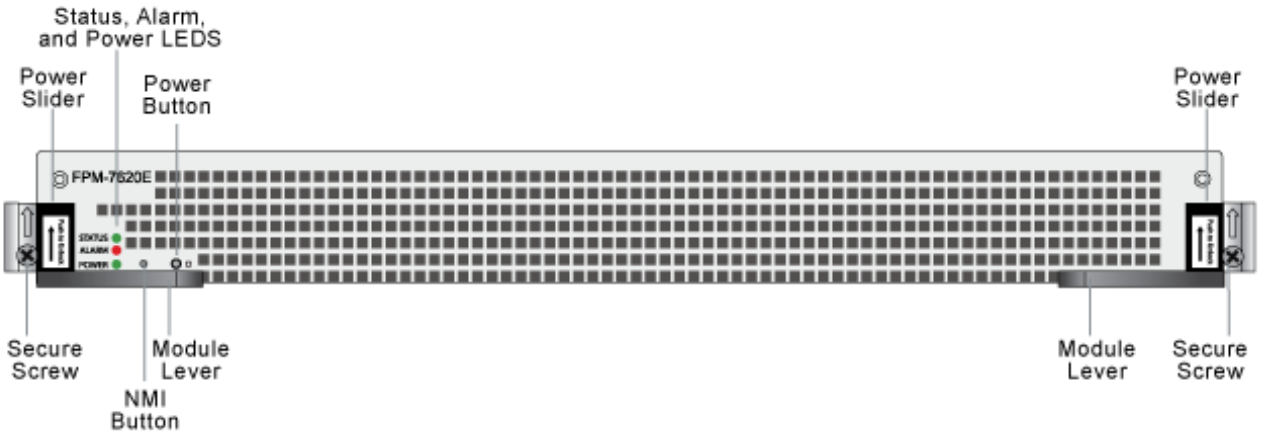
The FPM-7620E processing module is a high-performance worker module that processes sessions load balanced to it by FortiGate-7000 series interface (FIM) modules over the chassis fabric backplane. The FPM-7620E can be installed in any FortiGate-7000 series chassis in slots 3 and up.

The FPM-7620E includes two 80Gbps connections to the chassis fabric backplane and two 1Gbps connections to the base backplane. The FPM-7620E processes sessions using a dual CPU configuration, accelerates network traffic processing with 4 NP6 processors and accelerates content processing with 8 CP9 processors. The NP6 network processors are connected by the FIM switch fabric so all supported traffic types can be fast path accelerated by the NP6 processors.

The FPM-7620E includes the following hardware features:

- Two 80Gbps fabric backplane channels for load balanced sessions from the FIMs installed in the chassis.
- Two 1Gbps base backplane channels for management, heartbeat and session sync communication.
- Dual CPUs for high performance operation.
- Four NP6 processors to offload network processing from the CPUs.
- Eight CP9 processors to offload content processing and SSL and IPsec encryption from the CPUs.

FPM-7620E front panel

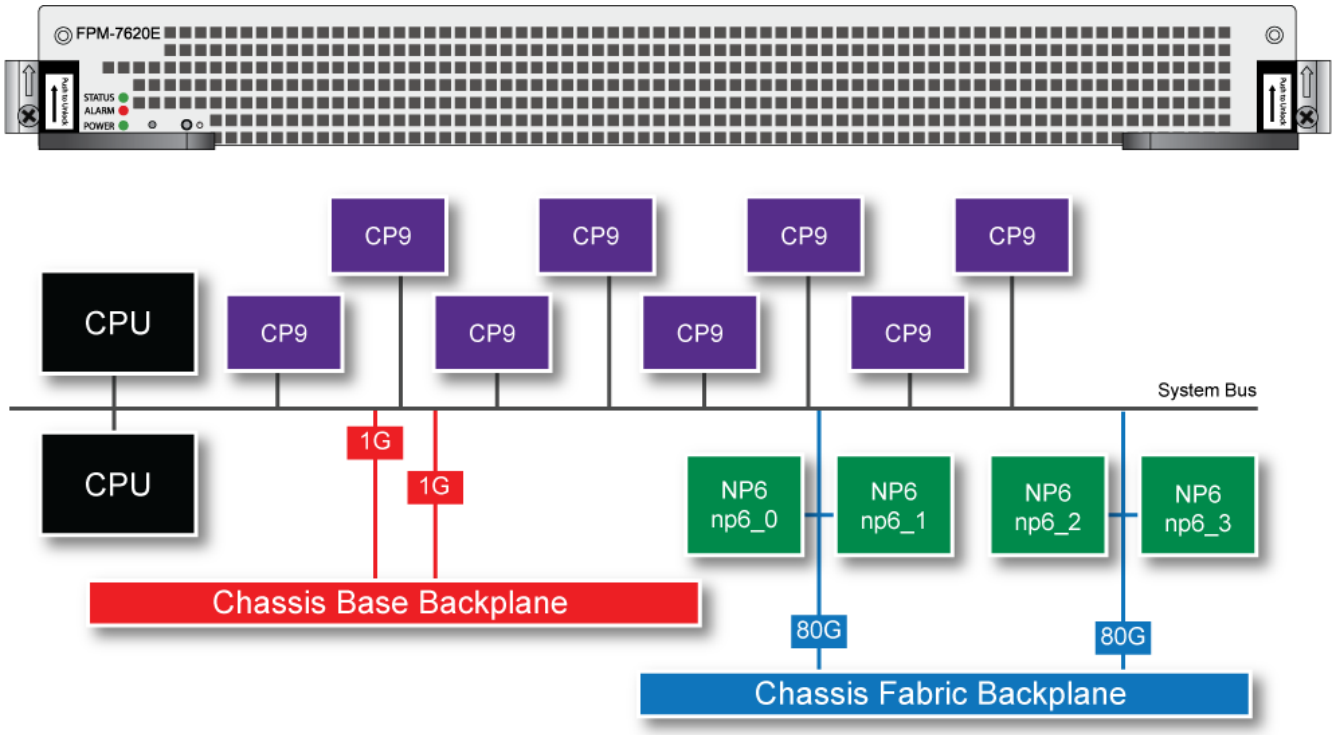


- Power button.
- NMI switch (for troubleshooting as recommended by Fortinet Support).
- Mounting hardware.
- LED status indicators.

NP6 network processors - offloading load balancing and network traffic

In a FortiGate-7000 chassis, FPM-7620E NP6 network processors combined with the FortiGate Interface Module (FIM) Integrated Switch Fabric (ISF) provide hardware acceleration by offloading sessions from the FPM-7620E CPUs. The result is enhanced network performance provided by the NP6 processors plus the removal of network processing load from the FPM-7620 CPUs. The NP6 processors can also handle some CPU-intensive tasks, like IPsec VPN encryption/decryption. Because of the ISF in each FIM, all sessions are fast-pathed and accelerated.

FPM-7620E hardware architecture



Accelerated IPS, SSL VPN, and IPsec VPN (CP9 content processors)

The FPM-7620E includes eight CP9 processors that provide the following performance enhancements:

- Flow-based inspection (IPS, application control etc.) pattern matching acceleration with over 10Gbps throughput
- IPS pre-scan
- IPS signature correlation
- Full match processors
- High performance VPN bulk data engine
- IPsec and SSL/TLS protocol processor
- DES/3DES/AES128/192/256 in accordance with FIPS46-3/FIPS81/FIPS197
- MD5/SHA-1/SHA256/384/512-96/128/192/256 with RFC1321 and FIPS180
- HMAC in accordance with RFC2104/2403/2404 and FIPS198
- ESN mode
- GCM support for NSA "Suite B" (RFC6379/RFC6460) including GCM-128/256; GMAC-128/256
- Key Exchange Processor that supports high performance IKE and RSA computation
- Public key exponentiation engine with hardware CRT support
- Primary checking for RSA key generation
- Handshake accelerator with automatic key material generation
- True Random Number generator
- Elliptic Curve support for NSA "Suite B"

- Sub public key engine (PKCE) to support up to 4096 bit operation directly (4k for DH and 8k for RSA with CRT)
- DLP fingerprint support
- TTTD (Two-Thresholds-Two-Divisors) content chunking
- Two thresholds and two divisors are configurable

Getting started with FortiGate-7000

Begin by installing your FortiGate-7000 chassis in a rack and installing FIM interface modules and FPM processing modules in it. Then you can power on the chassis and all modules in the chassis will power up.

Whenever a chassis is first powered on, it takes about 5 minutes for all modules to start up and become completely initialized and synchronized. During this time the chassis will not allow traffic to pass through and you may not be able to log into the GUI, or if you manage to log in the session could time out as the FortiGate-7000 continues negotiating.

Review the PSU, fan tray, management module, FIM, and FPM LEDs to verify that everything is operating normally. Wait until the chassis has completely started up and synchronized before making configuration changes.

You can use the `diagnose sys ha status` command to confirm that the FortiGate-7000 is completely initialized. If the output from entering this command hasn't changed after checking for a few minutes you can assume that the system has initialized. You don't normally have to confirm that the system has initialized, but this diagnose command is available for verification.

When the system has initialized, you have a few options for connecting to the FortiGate-7000 GUI or CLI:

- Log in to the GUI by connecting the MGMT1 interface of the FIM in slot 1 to your network. Then browse to https://192.168.1.99.
- Log in to the CLI by connecting the MGMT1 interface of the FIM in slot 1 to your network. Then use an SSH client to connect to 192.168.1.99 and use the same admin account to log in.
- Log in to the primary FIM CLI by connecting to the RJ-45 RS-232 Console 1 serial port on the FortiGate-7000 management module with settings: BPS: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.

The FortiGate-7000 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-7000 to your network.
MGMT1 IP/Netmask	192.168.1.99/24

All configuration changes must be made from the primary FIM GUI or CLI and not from the backup FIM or the FPMs.

All other management communication (for example, SNMP queries, remote logging, and so on) use the management aggregate interface and are handled by the primary FIM.

Default VDOM configuration and configuring the mgmt interface

The default FortiGate-7000 configuration includes a management VDOM named **mgmt-vdom**. The management interface (mgmt) and the HA heartbeat interfaces (M1 and M2) 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, the mgmt interface IP address, and so on.

Confirming startup status

Before verifying normal operation and making configuration changes and so on you should wait until the FortiGate-7000 is completely started up and synchronized. This can take a few minutes.

To confirm that the FortiGate-7000 is synchronized, view the **Security Fabric** dashboard widget. If the system is synchronized, the FIMs and FPMs should be visible and ForGate telemetry status should be **Connected**. The widget also indicates if any modules 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-7040E 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 FIMs and FPMs. If all of the FIMs and FPMs are synchronized, each output line should include `in_sync=1`. If a line ends with `in_sync=0`, that FIM or FPM is not synchronized. The following example just shows a few output lines:

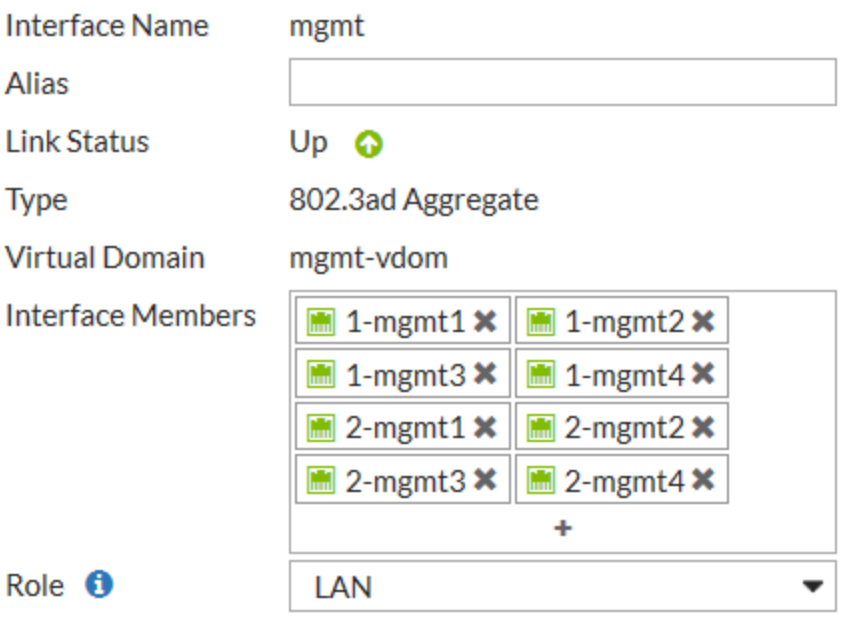
```
diagnose sys confsync status | grep in_sy
FIM10E3E16000062, Slave, uptime=53740.68, priority=2, slot_id=2:2, idx=3, flag=0x10, in_sync=1
FIM04E3E16000010, Slave, uptime=53790.94, priority=3, slot_id=1:1, idx=0, flag=0x10, in_sync=1
FIM04E3E16000014, Master, uptime=53781.29, priority=1, slot_id=2:1, idx=1, flag=0x10, in_sync=1
FIM10E3E16000040, Slave, uptime=53707.36, priority=4, slot_id=1:2, idx=2, flag=0x10, in_sync=1
FPM20E3E16900234, Slave, uptime=53790.98, priority=16, slot_id=2:3, idx=4, flag=0x64, in_sync=1
FPM20E3E16900269, Slave, uptime=53783.67, priority=17, slot_id=2:4, idx=5, flag=0x64, in_sync=1
FPM20E3E17900113, Slave, uptime=53783.78, priority=116, slot_id=1:3, idx=6, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=53784.11, priority=117, slot_id=1:4, idx=7, flag=0x64, in_sync=1
...
```

Setting up management connections

When your FortiGate-7000 first starts up, the MGMT1 to MGMT4 interfaces of both of the FIMs are part of a static 802.3 aggregate interface with a default IP address of 192.168.1.99. On the GUI or CLI the 802.3 aggregate interface is

named **mgmt**.

Example mgmt interface configuration



Setting up a single management connection

You can configure and manage your FortiGate-7000 by connecting an Ethernet cable to any of the MGMT1 - 4 interfaces of the FIM in slot 1 or slot 2 and logging into the GUI using HTTPS or the CLI using SSH. Usually you would connect to the MGMT1 interface.

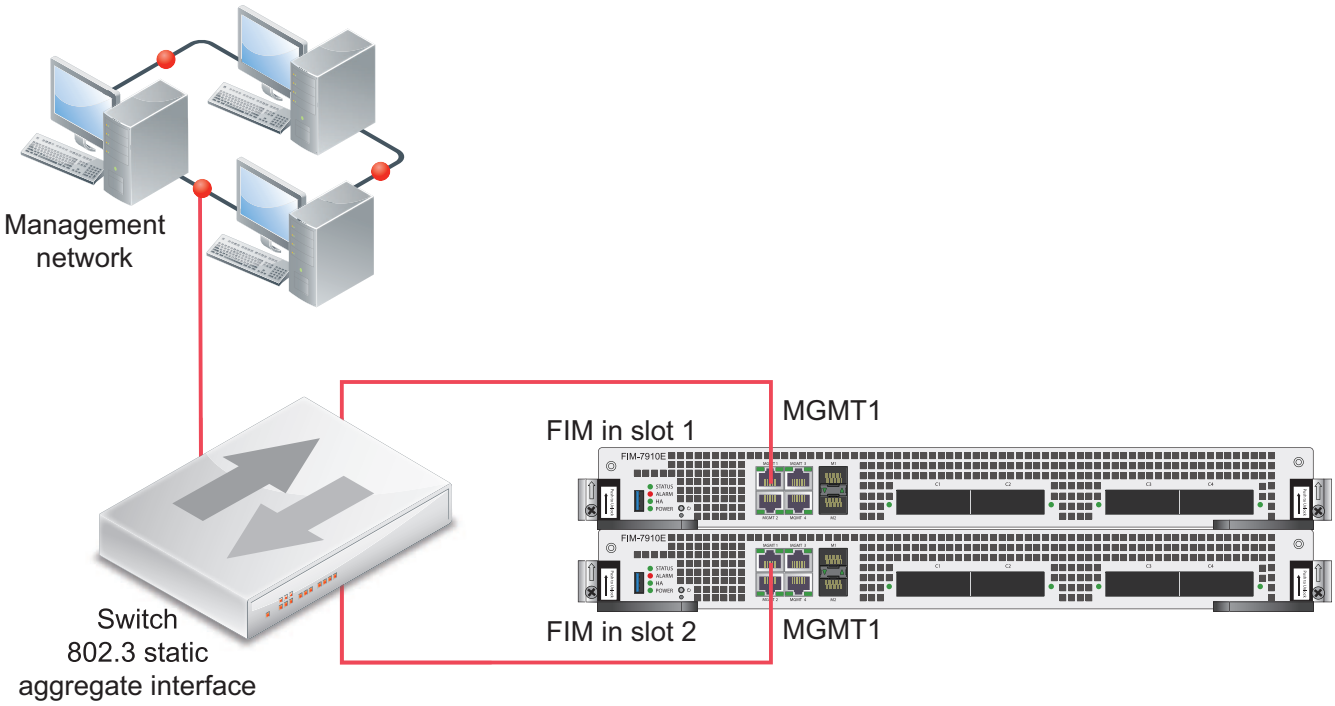
Setting up redundant management connections

You can set up redundant management connections to your FortiGate-7000 by adding a static 802.3 aggregate interface to a switch and setting up multiple connections between the switch and the FIM MGMT ports. Then connect the switch to your network.

LACP is not supported for the mgmt aggregate interface.

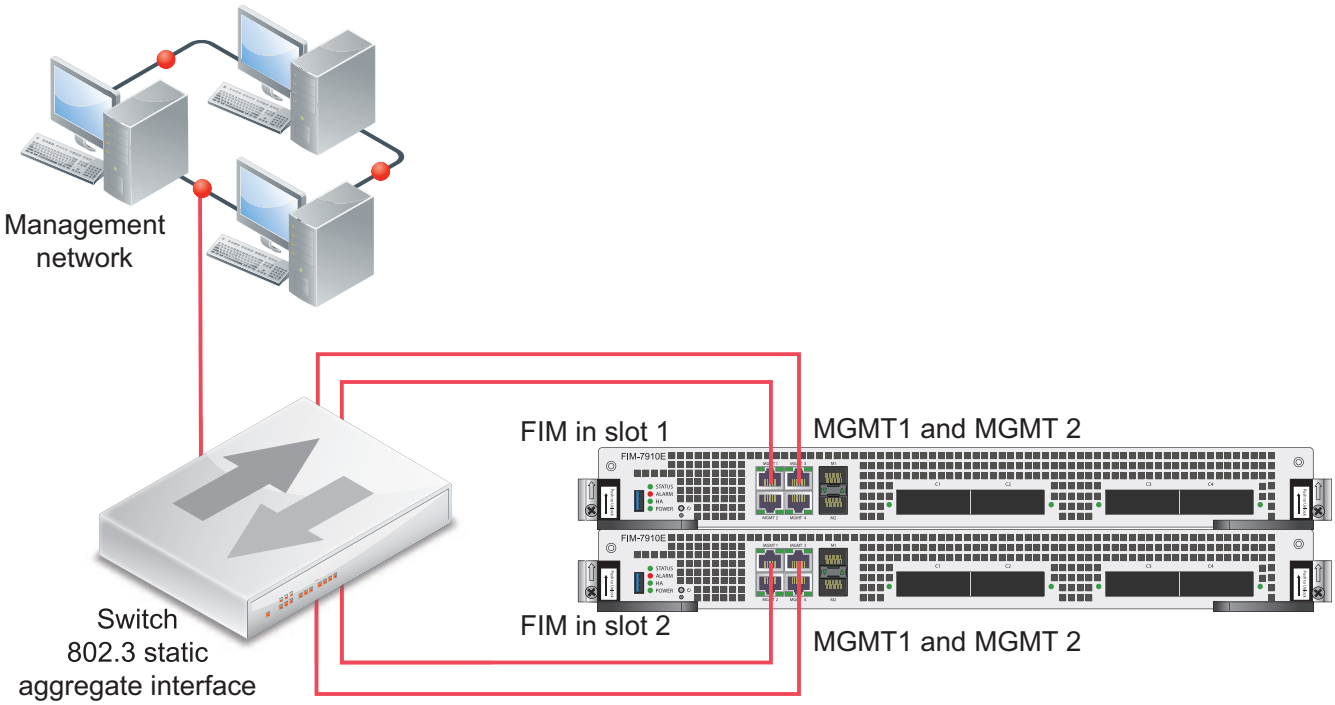
You do not have to change the configuration of the FortiGate-7000 to set up redundant management connections. The following example shows connections between the MGMT1 interfaces of each FIM to a switch. The switch is configured with a 802.3 static aggregate interface that includes two ports, one for each MGMT1 interface. The switch also connects the MGMT1 interfaces to a management network.

Example FortiGate-7000 redundant management connections



The following example shows redundant connections between both FIMs and the switch. In this case you need to add more switch ports to the static aggregate interface on the switch. You do not have to change the configuration of the FortiGate-7000 to set up this redundant management connection configuration.

Example FortiGate-7000 redundant management connections with redundant connections to each FIM



In either of these configurations, for additional redundancy you can use two switches. If you use two redundant switches, the static aggregate interface should span across both switches.

Configuration synchronization

Wen you log into the FortiGate-7000 GUI or CLI by connecting to the IP address of the aggregate management interface, or through a console connection, you are logging into the FIM in slot 1 (the address of slot 1 is FIM01). The FIM in slot 1 is the FortiGate-7000 config-sync master. All configuration changes must be made from the GUI or CLI of the FIM in slot 1. The he FIM in slot 1 synchronizes configuration changes to the other modules and makes sure module configurations remain synchronized with the FIM in slot 1.

If the FIM in slot 1 fails or reboots, the FIM in slot 2 becomes the config-sync master.

Once you have logged into the GUI or CLI of the FIM in slot 1 and verified that the system is operating normally, you can view and change the configuration of your FortiGate-7000 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-7000 dashboard widgets

The FortiGate-7000 includes a number of custom dashboard widgets that provide extra or custom information for FortiGate-7000 systems.

Security Fabric

The **Security Fabric** widget shows the FIMs and FPMs in your FortiGate-7000 system. You can hover over the components in the Security Fabric widget to see each components host name, serial number, model, firmware version, and management IP address. The Security Fabric widget also indicates if the modules are synchronized and communicating with the primary (master) FIM identifies the primary (master) FPM.

Interface Bandwidth

You can create multiple **Interface Bandwidth** widgets to show traffic that is transmitted and received by any FortiGate-7000 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, log rate, memory use, session creation rate, and the number of active sessions. You can create separate widgets for management traffic and data traffic. After you have crated 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** 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-7000 supports basic management communication through the FortiGate-7000 FIM front panel data interfaces. To enable management connections to these interfaces, configure the VDOM that the data interfaces are included in to allow traffic forwarding to the primary FIM.

For example, to allow management communication for interfaces in the root VDOM, edit the root VDOM from the CLI and enable both `icmp` and `admin`:

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

The `icmp` option is enabled by default and allows you to log into primary FIM 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 to 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 FIMs and FPMs

In some cases you may want to connect to individual modules. For example, you may want to view the traffic being processed by a specific FPM. You can connect to the GUI or CLI of individual modules in the FortiGate-7000 using the mgmt interface IP address with a special port number.

For example, if the mgmt interface IP address is 192.168.1.99, you can connect to the GUI of the FPM in slot 3 using the mgmt interface IP address followed by the special port number, for example:

`https://192.168.1.99:44303`

The special port number (in this case 44303) is a combination of the service port (for HTTPS, the service port is 443) and the chassis slot number (in this example, 03). The following table lists the special ports to use to connect to each FortiGate-7000 slot using common management protocols:

FortiGate-7000 special management port numbers

Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
5	FPM05	8005	44305	2305	2205	16105

Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
3	FPM03	8003	44303	2303	2203	16103
1	FIM01	8001	44301	2301	2201	16101
2	FIM02	8002	44302	2302	2202	16102
4	FPM04	8004	44304	2304	2204	16104
6	FPM06	8006	44306	2306	2206	16106

For example, to connect to the GUI of the FIM in slot 2 using HTTPS you would browse to https://192.168.1.99:44302.

To verify which module 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 modules allows you to use FortiView or Monitor GUI pages to view the activity of that module. Even though you can log in to different modules, you can only make configuration changes from the primary FIM; which is the FIM in slot 1.

Managing individual modules from the CLI

From the any CLI, you can use the `execute load-balance slot manage [<chassis>.]<slot>` command to log into the CLI of different FIMs and FPMs. You can use this command to view the status or configuration of the module, restart the module, or perform other operations. You should not change the configuration of individual FIMs or FPMs 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.

For example, in a FortiGate-7040E standalone configuration, if you have logged in to the CLI of the FIM in slot 1, enter the following command to log in to the FPM in slot 4:

```
execute load-balance slot manage 4
```

In a FortiGate-7040E HA configuration, if you logged into the CLI of the FIM in slot 1 chassis 1, enter the following command to log into the FPM in chassis 2 slot 4:

```
execute load-balance slot manage 2.4
```

In a FortiGate-7060E HA configuration, if you logged in to the CLI of the FIM in slot 1 chassis 2, enter the following command to log in to the FPM 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 FIM in slot 1 chassis 1, enter the following command to log in to the FPM in slot 3 of the same chassis:

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

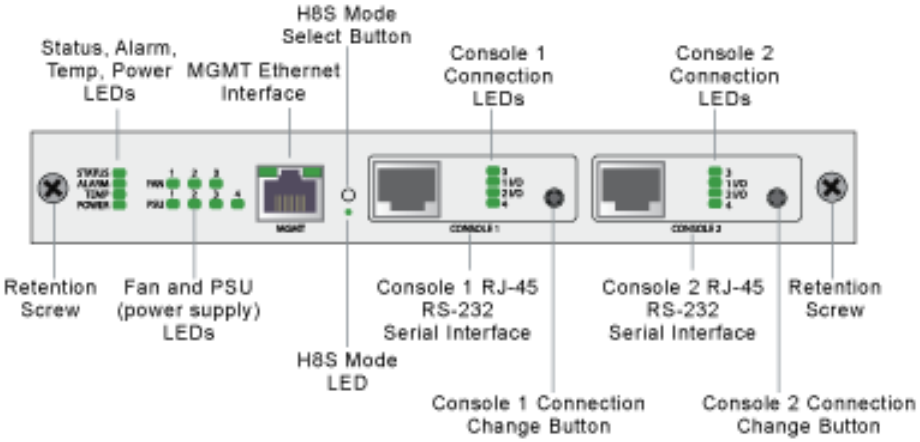
After you log in to a different module in this way, you can't use the `execute load-balance slot manage` command to log in to another module. Instead you must use the `exit` command to revert back to the CLI of the

component that you originally logged in to. Then, you can use the `execute load-balance slot manage` command to log into another module.

Connecting to module CLIs using the management module

All FortiGate-7000 chassis includes a management module (also called a shelf manager) on the chassis front panel. See the system guide for your chassis for details about the management module.

ForiGate-7040E management module front panel



The management module includes two console ports named Console 1 and Console 2 that can be used to connect to the CLI of the FIM and FPMs in the chassis. As described in the system guide, the console ports are also used to connect to SMC CLIs of the management module and the FIMs and FPMs

By default when the chassis first starts up Console 1 is connected to the FortiOS CLI of the FIM in slot 1 and Console 2 is disconnected. The default settings for connecting to each console port are:

Baud Rate (bps) 9600, Data bits 8, Parity None, Stop bits 1, and Flow Control None.

You can use the console connection change buttons to select the CLI that each console port is connected to. Press the button to cycle through the FIM and FPM FortiOS CLIs and disconnect this console. The console's LEDs indicate what it is connected to. If no LED is lit the console is either connected to the management module SMC SDI console or disconnected. Both console ports cannot be connected to the same CLI at the same time. If a console button press would cause a conflict that module is skipped. If one of the console ports is disconnected then the other console port can connect to any CLI.

If you connect a PC to one of the management module console ports with a serial cable and open a terminal session you can press **Ctrl-T** to enable console switching mode. Press Ctrl-T multiple times to cycle through the FIM and FPM module FortiOS CLIs (the new destination is displayed in the terminal window). If you press **Ctrl-T** after connecting to the FPM module in slot 6 the console is disconnected. Press Ctrl-T again to start over again at slot 1.

Example: connecting to the FortiOS CLI of the FIM in slot 1

Use the following steps to connect to the FortiOS CLI of the FpM in slot 3:

1. Connect the console cable supplied with your chassis to Console 1 and to your PC or other device RS-232 console port.
2. 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.
3. Press **Ctrl-T** to enter console switch mode.
4. Repeat pressing **Ctrl-T** until you have connected to slot 1. Example prompt:
   `<Switching to Console: FPM03 (9600)>`
5. Log in to the CLI.
6. When your session is complete, enter the `exit` command to log out or use Ctrl-T to switch to another module CLI.

Firmware upgrades

All of the FIMs and FPMs in your FortiGate-7000 system run the same firmware image. You upgrade the firmware using the primary FIM GUI or CLI just as you would any FortiGate product. During the upgrade process, the firmware running on all of the FIMs and FPMs upgrades in one step. Firmware upgrades should be done during a quiet time because traffic will be briefly interrupted by the upgrade process. The entire firmware upgrade takes a few minutes. depending on the number of FIMs and FPMs in your FortiGate-7000 system. Some firmware upgrades may take longer depending on other factors, such as the size of the configuration and whether a DP processor firmware upgrade 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-7000 configuration.

Fortinet recommends that you review the services provided by your FortiGate-7000 before a firmware upgrade and then again after the upgrade to make sure the services continues 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
```

Verifying that a firmware upgrade is successful

After a FortiGate-7000 firmware upgrade, you should verify that all of the FIMs and FPMs have been successfully upgraded to the new firmware version.

After the firmware upgrade appears to be complete:

1. Log into the primary FIM and verify that it is running the expected firmware version.
   You can verify the firmware version running on the primary FIM from the dashboard or by using the `get system status` command.
   You can also use the `diagnose sys confsync status | grep in_sy` command to see if the FIMs and FPMs are all synchronized. In the command output `in_sync=1` means the FIM or FPM is synchronized. `In_sync=0` means the FIM or FPM is not synchronized, which could indicated the FIM or FPM is running a different firmware build than the primary FIM.
2. Log into the other FIMs and the FPMs, and in the same way confirm that they are also running the expected firmware version.
   You can log into individual FIMs or FPMs using the system management IP address and the special port number for each module. For example, https://192.268.1.99:44303 connects to the FPM in slot 3. The special port number (in this case 44303) is a combination of the service port (for HTTPS the service port is 443) and the slot number (in this example, 03).
   If you are using a management module console port to connect to the primary FIM CLI you can use Ctrl-T to switch between the CLIs of each of the modules.

Installing firmware on individual FIMs and FPMs

You can install firmware on individual FIMs or FPMs by logging into the FIM or FPM GUI or CLI. You can also setup a console connection to the FortiGate-7000 front panel Management Module and install firmware on individual FIMs or FPMs from a TFTP server after interrupting the FIM or FPM boot up sequence from the BIOS.

Normally you wouldn't need to upgrade the firmware on individual FIMs or FPMs because the FortiGate-7000 keeps the firmware on all of the FIMs and FPMs synchronized. However, FIM or FPM firmware may go out of sync in the following situations:

- Communication issues during a normal FortiGate-7000 firmware upgrade.
- Installing a replacement FIM or FPM that is running a different firmware version.
- Installing firmware on or formatting an FIM or FPM from the BIOS.

To verify the firmware versions on each FIM or FPM you can check individual FIM and FPM GUIs or enter the `get system status` command from each FIM or FPM CLI. You can also use the `diagnose sys confsync status | grep in_sy` command to see if the FIMs and FPMs are all synchronized. In the command output, `in_sync=1` means the FIM or FPM is synchronized. `In_sync=0` means the FIM or FPM is not synchronized, which could indicated the FIM or FPM is running a different firmware build than the primary FIM.

The procedures in this section work for FIMs or FPMs in a standalone FortiGate-7000. These procedures also work for FIMs or FPMs in the primary FortiGate-7000 in an HA configuration. To upgrade firmware on an FIM or FPM in the backup FortiGate-7000 in an HA configuration, you should either remove the backup FortiGate-7000 from the HA configuration or cause a failover so that the backup FortiGate-7000 becomes the primary FortiGate-7000.

In general, if you need to update both FIMs and FPMs in the same FortiGate-7000, you should update the FIMs first as the FPMs can only communicate through FIM interfaces.

Upgrading FIM firmware

Use the following procedure to upgrade the firmware running on a single FIM. For this procedure to work, you must connect at least one of the FIM MGMT interfaces to a network. You must also be able to log in to the FIM GUI or CLI from that MGMT interface. If you perform the firmware upgrade from the CLI, the FIM must be able to communicate with an FTP or TFTP server.

During the upgrade, the FIM will not be able to process traffic. However, the other FIM and the FPMs should continue to operate normally.

1. Log into the FIM GUI or CLI and perform a normal firmware upgrade.
   You may need to use the special port number to log in to the FIM in slot two (for example, browse to https://192.168.1.99:44302).
2. Once the FIM restarts, verify that the new firmware has been installed.
   You can do this from the FIM GUI dashboard or from the FIM CLI using the `get system status` command.
3. Verify that the configuration has been synchronized to the upgraded FIM. The following command output shows the synchronization status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_
sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=1
```

   FIMs and FPMs that are missing or that show `in_sync=0` are not synchronized. To synchronize an FIM or FPM that is not synchronized, log into the CLI of the FIM or FPM 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 FIM in slot 2 is lower than the uptime of the other modules, indicating that the FIM in slot 2 has recently restarted.

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

Upgrading FPM firmware

Use the following procedure to upgrade the firmware running on an individual FPM. To perform the upgrade, you must enter a command from the primary FIM CLI to allow ELBC communication with the FPM. Then you can just log in to the FPM GUI or CLI and perform the firmware upgrade.

During this procedure, the FPM will not be able to process traffic. However, the other FPMs and the FIMs should continue to operate normally.

After verifying that the FPM is running the right firmware, you must log back into the primary FIM CLI and return the FPM to normal operation.

1. Log in to the primary FIM CLI and enter the following command:
   `diagnose load-balance switch set-compatible <slot> enable elbc`
   Where `<slot>` is the number of the FortiGate-7000 slot containing the FPM to be upgraded.
2. Log in to the FPM GUI or CLI using its special port number (for example, for the FPM in slot 3, browse to https://192.168.1.99:44303 to connect to the GUI) and perform a normal firmware upgrade of the FPM.
3. After the FPM restarts, verify that the new firmware has been installed.
   You can do this from the FPM GUI dashboard or from the FPM CLI using the `get system status` command.
4. Verify that the configuration has been synchronized. The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_
sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=1
```

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

   The command output also shows that the uptime of the FPM in slot 4 is lower than the uptime of the other modules, indicating that the FPM in slot 4 has recently restarted.

   If you enter the `diagnose sys confsync status | grep in_sy` command before the FIM has completely restarted, it will not appear in the command output. As well, the Security Fabric dashboard widget will temporarily show that it is not synchronized.
5. Once the FPM is operating normally, log back in to the primary FIM CLI and enter the following command to reset

the FPM to normal operation:

```
diagnose load-balance switch set-compatible <slot> disable
```

Configuration synchronization errors will occur if you do not reset the FPM to normal operation.

Upgrading FIM firmware from the FIM BIOS using a TFTP server

Use the following procedure to upload firmware from a TFTP server to an FIM. The procedure involves creating a connection between the TFTP server and one of the FIM MGMT interfaces. You don't have to use a MGMT interface on the FIM that you are upgrading.

This procedure also involves connecting to the FIM CLI using a FortiGate-7000 front panel Management Module console port. From the console session, the procedure describes how to restart the FIM, interrupting the boot process, and follow FIM BIOS prompts to install the firmware.

During this procedure, the FIM will not be able to process traffic. However, the other FIM and the FPMs should continue to operate normally.

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 FIM MGMT interfaces.

   If the MGMT interface you are using is one of the MGMT interfaces connected as a LAG to a switch, you must shutdown or disconnect all of the other connections in the LAG from the switch. This includes the MGMT interfaces in the other FIM.
3. Using the console cable supplied with your FortiGate-7000, connect the management module Console 1 port on the FortiGate-7000 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. Press Ctrl-T to enter console switch mode.
6. Repeat pressing Ctrl-T until you have connected to the FIM to be updated. Example prompt for the FIM in slot 2:

   `<Switching to Console: FIM02 (9600)>`
7. Optionally log in to the FIM's CLI.
8. Reboot the FIM.

   You can do this using the `execute reboot` command from the CLI or by pressing the power switch on the FIM front panel.
9. When the FIM starts up, follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.
10. To set up the TFTP configuration, press C.
11. 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 must not be the same as the FortiGate-7000 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.

12. To quit this menu, press Q.
13. 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.
14. To start the TFTP transfer, press T.
    The firmware image is uploaded from the TFTP server and installed on the FIM. The FIM then restarts with its configuration reset to factory defaults. After restarting, the FIM configuration is synchronized to match the configuration of the primary FIM. The FIM restarts again and can start processing traffic.
15. Once the FIM restarts, verify that the correct firmware is installed.
    You can do this from the FIM GUI dashboard or from the FPM CLI using the `get system status` command.
16. Verify that the configuration has been synchronized.
    The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_
sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FIM10E3E16000040, Slave, uptime=346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=1
```

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

    The command output also shows that the uptime of the FIM in slot 2 is lower than the uptime of the other modules, indicating that the FIM in slot 2 has recently restarted.

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

Upgrading FPM firmware from the FPM BIOS using a TFTP server

Use the following procedure to upload firmware from a TFTP server to an FPM. To perform the upgrade, you must enter a command from the primary FIM CLI to allow the FPM BIOS to communicate through an FIM MGMT interface. The procedure involves creating a connection between the TFTP server and one of the FIM MGMT interfaces.

This procedure also involves connecting to the FPM CLI using a FortiGate-7000 front panel Management Module console port, rebooting the FPM, interrupting the boot from the console session, and following FPM BIOS prompts to install the firmware.

During this procedure, the FPM will not be able to process traffic. However, the other FPMs and the FIMs should continue to operate normally.

After you verify that the FPM is running the right firmware, you must log back in to the primary FIM CLI and return the FPM to normal operation.

1. Set up a TFTP server and copy the firmware file into the TFTP server default folder.
2. Log into to the primary FIM CLI and enter the following command:
   `diagnose load-balance switch set-compatible <slot> enable bios`
   Where `<slot>` is the number of the FortiGate-7000 slot containing the FPM to be upgraded.
3. Set up your network to allow traffic between the TFTP server and a MGMT interface of one of the FIMs.
   You can use any MGMT interface of either of the FIMs. If the MGMT interface you are using is one of the MGMT interfaces connected as a LAG to a switch you must shutdown or disconnect all of the other connections in the LAG from the switch. This includes the MGMT interfaces in the other FIM.
4. Using the console cable supplied with your FortiGate-7000, connect the management module Console 1 port on the FortiGate-7000 to the RS-232 port on your management computer.
5. 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.
6. Press Ctrl-T to enter console switch mode.
7. Repeat pressing Ctrl-T until you have connected to the module to be updated. Example prompt:
   `<Switching to Console: FPM03 (9600)>`
8. Optionally log into the FPM's CLI.
9. Reboot the FPM.
   You can do this using the `execute reboot` command from the FPM's CLI or by pressing the power switch on the FPM front panel.
10. When the FPM starts up, follow the boot process in the terminal session and press any key when prompted to interrupt the boot process.
11. To set up the TFTP configuration, press C.
12. 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 must not be the same as the FortiGate-7000 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.
13. To quit this menu, press Q.
14. 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.
15. To start the TFTP transfer, press T.
    The firmware image is uploaded from the TFTP server and installed on the FPM. The FPM then restarts with its configuration reset to factory defaults. After restarting, the FPM configuration is synchronized to match the

configuration of the primary FPM. The FPM restarts again and can start processing traffic.

16. Once the FPM restarts, verify that the correct firmware is installed.
    You can do this from the FPM GUI dashboard or from the FPM CLI using the `get system status` command.
17. Verify that the configuration has been synchronized.
    The following command output shows the sync status of a FortiGate-7040E. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_
sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
sync=1
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
sync=1
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
sync=1
FPM20E3E17900217, Slave, uptime=387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=1
```

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

    The command output also shows that the uptime of the FPM in slot 4 is lower than the uptime of the other modules, indicating that the FPM in slot 4 has recently restarted.

    If you enter the `diagnose sys confsync status | grep in_sy` command before the FPM has restarted, it will not appear in the command output. As well, the Security Fabric dashboard widget will temporarily show that it is not synchronized.
18. Once the FPM is operating normally, log back in to the primary FIM CLI and enter the following command to reset the FPM to normal operation:
    `diagnose load-balance switch set-compatible <slot> disable`
    Configuration synchronization errors will occur if you do not reset the FPM to normal operation.

Synchronizing FIMs and FPMs after upgrading the primary FIM firmware from the BIOS

After you install firmware on the primary FIM from the BIOS after a reboot, the firmware version and configuration of the primary FIM will most likely be not be synchronized with the other FIMs and FPMs. You can verify this from the primary FIM CLI using the `diagnose sys confsync status | grep in_sy` command. The `in_sync=0` entries in the following example output show that the management board (serial number ending in 10) is not synchronized with the other FIM and the FPMs shown in the example.

```
diagnose sys confsync status | grep in_sy
FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_sync=0
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
sync=0
FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
...
```

You can also verify synchronization status from primary FIM Security Fabric dashboard widget.

To re-synchronize the FortiGate-7000, which has the effect of resetting the other FIM and the FPMs, re-install firmware on the primary FIM.

You can also manually install firmware on each individual FIM and FPM from the BIOS after a reboot. This manual process is just as effective as installing the firmware for a second time on the primary FIM to trigger synchronization to the FIM and the FPMs, but takes much longer.

1. Log into the primary FIM GUI.
2. Install a firmware build on the primary FIM from the GUI or CLI. The firmware build you install on the primary FIM can either be the same firmware build or a different one.

   Installing firmware synchronizes the firmware build and configuration from the primary FIM to the other FIM and the FPMs.
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 ForGate-7040E shows that the primary FIM is synchronized with the other FIM and all of the FPMs because each line includes in_sync=1:

   ```
   diagnose sys confsync status | grep in_sy
   FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
   sync=1
   FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
   sync=1
   FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
   sync=1
   FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x4, in_
   sync=1
   FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
   sync=1
   FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
   sync=1
   FIM04E3E16000010, Master, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_
   sync=1
   FIM10E3E16000040, Slave, uptime=69346.99, priority=2, slot_id=1:2, idx=1, flag=0x0, in_
   sync=1
   FPM20E3E17900217, Slave, uptime=69387.74, priority=20, slot_id=1:4, idx=2, flag=0x64, in_
   sync=1
   ```

Restarting the FortiGate-7000

To restart all of the modules in a FortiGate-7000 chassis, connect to the primary FIM CLI and enter the `execute reboot` command. When you enter this command from the primary FIM, all of the modules restart.

To restart individual FIMs or FPMs, log in to the CLI of the module to restart and run the `execute reboot` command.

Failover in a standalone FortiGate-7000

A FortiGate-7000 will continue to operate even if an FIM or FPM fails or is removed. If an FPM fails, sessions being processed by that FPM fail and must be restarted. All sessions are load balanced to the remaining FPMs.

If an FIM fails, the other FIM will continue to operate and will become the config-sync master. However, traffic received or sent by the interfaces of failed FIM will be lost.

You can use LACP or redundant interfaces to connect interfaces of both FIMs to the same network. In this way, if one of the FIMs fails the traffic will continue to be received by the other FIM.

Replacing a failed FPM or FIM

This section describes how to remove a failed FPM or FIM and replace it with a new one. The procedure is slightly different depending on if you are operating in HA mode with two FortiGate-7000s or just operating a standalone FortiGate-7000.

Replacing a failed module in a standalone FortiGate-7000

1. Power down the failed module by pressing the front panel power button.
2. Remove the module from the chassis.
3. Insert the replacement module. It should power up when inserted into the chassis if the chassis has power.
4. The module's configuration is synchronized and its firmware is upgraded to match the firmware version on the primary FIM. The new module reboots.
5. Confirm that the new module is running the correct firmware version either from the GUI or by using the `get system status` command.

   Manually update the module to the correct version if required. You can do this by logging into the module and performing a firmware upgrade. See Installing firmware on individual FIMs and FPMs on page 41.
6. Use the `diagnose sys confsync status | grep in_sy` command to confirm that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the modules are synchronized.

   If `in_sync` is not equal to 1, or if a module is missing in the command output you can try restarting the modules in the chassis by entering execute reboot from any module CLI. If this does not solve the problem, contact Fortinet Support.

Replacing a failed module in a FortiGate-7000 chassis in an HA cluster

1. Power down the failed module by pressing the front panel power button.
2. Remove the module from the chassis.
3. Insert the replacement module. It should power up when inserted into the chassis if the chassis has power.
4. The module's configuration is synchronized and its firmware is upgraded to match the configuration and firmware version on the primary module. The new module reboots.
5. Confirm that the module is running the correct firmware version.
   Manually update the module to the correct version if required. You can do this by logging into the module and performing a firmware upgrade.
6. Configure the new module for HA operation. For example:
   ```
   config system ha
      set mode a-p
      set chassis-id 1
      set hbdev m1 m2
      set hbdev-vlan-id 999
      set hbdev-second-vlan-id 990
   ```
   end
7. Optionally configure the hostname:
   ```
   config system global
      set hostname <name>
   end
   ```
   The HA configuration and the hostname must be set manually because HA settings and the hostname is not synchronized.
8. Use the `diagnose sys confsync status | grep in_sy` command to confirm that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the modules are synchronized.
   If `in_sync` is not equal to 1, or if a module is missing in the command output you can try restarting the modules in the chassis by entering execute reboot from any module CLI. If this does not solve the problem, contact Fortinet Support.

Packet sniffing for FIM and FPM packets

From a VDOM, you can use the `diagnose sniffer packet` command to view or sniff packets as they are processed by FIM or FPMs for that VDOM. To use this command you have to be logged into a VDOM. You can run this command from any FIM or FPM CLI.

The command output includes the address of the slot containing the module that processed the packet. From the primary FIM, you can see packets processed by all of the FIMs and FPMs. From individual FIMs or FPMs you can see packets processed by that FIM or FPM.

From the primary FIM, you can enter the `diagnose sniffer options slot currrent` command to only see packets processed by the primary FIM. You can also enter the `diagnose sniffer options slot default` command to see packets processed by all modules.

The command syntax is:

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

Where:

<interface> is the name of one or more interfaces on which to sniff for packets. Use any to sniff packets for all interfaces. To view management traffic use the elbc-base-ctrl interface name.

<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.

Sample diagnose sniffer packet output from the primary FIM

```
[FPM04] 1.598890 3ffe:1:1:4::97b.13344 -> 3ffe:1:2:4::105.25: syn 151843506
[FPM03] 1.214394 802.1Q vlan#4022 P0 3ffe:1:1:2::214.10012 -> 3ffe:1:2:2::103.53: udp 30
[FIM02] 2.177930 llc unnumbered, 23, flags [poll], length 40
[FIM01] 1.583778 172.30.248.99.57167 -> 10.160.19.70.443: ack 2403720303
[FPM04] 1.598891 17.3.8.3.14471 -> 18.3.1.107.143: syn 2715027438 ^C
[FPM03] 1.214395 3ffe:1:1:2::214.10012 -> 3ffe:1:2:2::103.53: udp 30
[FIM01] 1.583779 172.30.248.99.57167 -> 10.160.19.70.443: ack 2403720303
```

Diagnose debug flow trace for FPM and FIM activity

The diagnose debug flow trace output from the FortiGate-7000 primary FIM CLI shows traffic from all FIMs and FPMs. Each line of output begins with the name of the component that produced the output. For example:

```
diagnose debug enable
[FPM04]  id=20085 trace_id=6 func=print_pkt_detail line=5777 msg="vd-root:0 received a packet(proto=6,
10.0.2.3:10001->20.0.0.100:80) from HA-LAG0. flag [S], seq 2670272303, ack 0, win 32768"
[FPM03]  id=20085 trace_id=7 func=print_pkt_detail line=5777 msg="vd-root:0 received a packet(proto=6,
10.0.2.3:10002->20.0.0.100:80) from HA-LAG0. flag [S], seq 3193740413, ack 0, win 32768"
[FPM04]  id=20085 trace_id=6 func=init_ip_session_common line=5937 msg="allocate a new session-0000074c"
[FPM04]  id=20085 trace_id=6 func=vf_ip_route_input_common line=2591 msg="find a route: flag=04000000 gw-
20.0.0.100 via HA-LAG1"
[FPM04]  id=20085 trace_id=6 func=fw_forward_handler line=755 msg="Allowed by Policy-10000:"
```

Running FortiGate-7000 diagnose debug flow trace commands from an individual FPM CLI shows traffic processed by that FPM only.

```
diagnose debug enable
[FPM03]  id=20085 trace_id=7 func=print_pkt_detail line=5777 msg="vd-root:0 received a packet(proto=6,
10.0.2.3:10002->20.0.0.100:80) from HA-LAG0. flag [S], seq 3193740413, ack 0, win 32768"
[FPM03]  id=20085 trace_id=7 func=init_ip_session_common line=5937 msg="allocate a new session-000007b2"
[FPM03]  id=20085 trace_id=7 func=vf_ip_route_input_common line=2591 msg="find a route: flag=04000000 gw-
20.0.0.100 via HA-LAG1"
[FPM03]  id=20085 trace_id=7 func=fw_forward_handler line=755 msg="Allowed by Policy-10000:"
```

Showing how the DP2 processor will load balance a session

You can use the following command to display the FPM slot that the DP2 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 FPM slot 2 by the DP2 processor.

```
diagnose load-balance dp find session normal 6 11.1.1.11 53386 12.1.1.11 22
================================================================================
MBD SN: F7KF503E17900068
Primary Bin 9708928
New session to slot 2 (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-7000 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-7000 IPsec VPN on page 66.

FortiGate-7000 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 53). 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 FPM.
2. TCP, UDP, SCTP, ICMP (IPv4 only) and ESP (IPv4 only) sessions that do not match a flow rule are directed to the DP2 processors.
   The DP2 processors distribute sessions to the FPMs 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) FPM.

Setting the load balancing method

Sessions are load balanced or distributed 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 FPMs 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 112.

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) FPM by configuring flow rules for that traffic. You can also configure flow rules to send traffic that cannot be load balanced to specific FPMs.

Create flow rules using the `config loadbalance 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 FPM. You can view the default configuration of the `config loadbalance flow-rule` command to see how this is all configured. For example, the following configuration sends BGP source and destination sessions to the primary FPM:

```
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 59 for a listing of all of the default flow rules.

Determining the primary FPM

You can use the `diagnose load-balance status` command to determine which FPM is operating as the primary FPM. The following example `diagnose load-balance status` output for a FortiGate-7060E showing that the FPM in slot 3 is the primary (master) FPM. The command output also shows the status of all of the FPMs in the FortiGate-7060E. The output also shows that the FPM in slot 4 is either missing or down.

```
diagnose load-balance status
================================================================================
Slot: 2  Module SN: FIM04E3E16000222
  FIM02: FIM04E3E16000222
  Master FPM Blade: slot-3

     Slot  3: FPM20E3E17900133
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  4:
       Status:Dead      Function:Active
```

```
Link:      Base: Up          Fabric: Down
Heartbeat: Management: Failed Data: Failed
Status Message:"Waiting for management heartbeat."
```

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

SSL VPN load balancing

FortiGate-7000s do not support load balancing SSL VPN sessions terminated by the FortiGate-7000. The recommended configuration is to direct SSL VPN sessions terminated by the FortiGate-7000 to the primary FPM.

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

Using a FortiGate-7000 as an SSL VPN server requires you to manually add an SSL VPN load balance flow rule to configure the FortiGate-7000 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 FPM"
   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 FPM. 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 FPM.

Adding the SSL VPN server IP address

You can add the IP address of the FortiGate-7000 interface that receives SSL VPN traffic to the SSL VPN flow rule to make sure that the flow rule only matches SSL VPN server settings. 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 FPM"
```

```
   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 FPM.

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 FPM"
   end
```

FortiOS Carrier GTP load balancing

if you are operating a FortiGate-7000 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-7000 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-7000 systems licensed for FortiOS Carrier load balance GTP-C traffic to all FPMs. 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) FPM, 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 FPM. Enabling this flow rule can reduce GTP performance, since all GTP-C tunnel setup sessions will be done by the primary FPM and not distributed among all of the FPMs.

```
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 FPMs. GTP-U load balancing uses Tunnel Endpoint Identifiers (TEIDs) to identify and load balance sessions.

ICMP load balancing

You can use the following option to configure load balancing for ICMP sessions:

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

The default setting is `to-master` and all ICMP traffic is sent to the primary (master) FPM.

If you want to load balance ICMP sessions to multiple FPMs, you can select one of the other options. You can load balance ICMP sessions by source IP address, by destination IP address, or by source and destination IP address.

You an also select `derived` to load balance ICMP sessions 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.

Adding a flow rule to support DHCP relay

The FortiGate-7000 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-7000 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-7000 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) FPM (`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 or FPM.

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
   set ipsec-load-balance enable
end
```

If you disable IP sec VPN load balancing by setting `ipsec-load-balance` to `disable`, the FortiGate-7000 automatically enables the IPsec VPN flow rules and sends all IPsec VPN traffic to the primary FPM.

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 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
    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-7000 IPsec VPN

FortiOS 6.0 for FortiGate-7000 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-7000 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-7000 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 FPMs is not supported. IPsec VPN load balancing should be disabled. By default, all IPsec VPN traffic is handled by the primary FPM.
- IPsec SA synchronization between HA peers is not supported. After an HA failover, IPsec VPN tunnels have to be re-initialized.

FortiGate-7000 IPsec VPN load balancing

Since the FortiGate-7000 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.

Troubleshooting

Use the following commands to verify that IPsec VPN sessions are up and running.

Use the `diagnose load-balance status` command from the primary FIM interface module to determine the primary FPM. For FortiGate-7000 HA, run this command from the primary FortiGate-7000. The third line of the command output shows which FPM is operating as the primary FPM.

```
diagnose load-balance status
  FIM01: FIM04E3E16000074
  Master FPM Blade: slot-4

     Slot  3: FPM20E3E17900113
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  4: FPM20E3E16800033
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
```

```
      Status Message:"Running"

  FIM02: FIM10E3E16000040
  Master FPM Blade: slot-4

     Slot  3: FPM20E3E17900113
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  4: FPM20E3E16800033
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
```

Log into the primary FPM CLI and from here log into the VDOM that you added the tunnel configuration to and run the command `diagnose vpn tunnel list <phase2-name>` to show the sessions for the phase 2 configuration. The example below is for the `to-fgt2` phase 2 configuration configured previously in this chapter. The command output shows the security association (SA) setup for this phase 2 and the all of the destination subnets .

From the command output, make sure the SA is installed and the `dst` addresses are correct.

```
CH15 [FPM04] (002ipsecvpn) # diagnose vpn tunnel list name to-fgt2
list ipsec tunnel by names in vd 11
------------------------------------------------------
name=to-fgt2 ver=1 serial=2 4.2.0.1:0->4.2.0.2:0
bound_if=199 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/40 options[0028]=npu ike_assit
proxyid_num=1 child_num=0 refcnt=8581 ilast=0 olast=0 auto-discovery=0
ike_asssit_last_sent=4318202512
stat: rxp=142020528 txp=147843214 rxb=16537003048 txb=11392723577
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=2
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to-fgt2 proto=0 sa=1 ref=8560 serial=8
  src: 0:4.2.1.0/255.255.255.0:0 0:4.2.2.0/255.255.255.0:0
  dst: 0:4.2.3.0/255.255.255.0:0 0:4.2.4.0/255.255.255.0:0 0:4.2.5.0/255.255.255.0:0
  SA: ref=7 options=22e type=00 soft=0 mtu=9134 expire=42819/0B replaywin=2048 seqno=4a26f
esn=0 replaywin_lastseq=00045e80
  life: type=01 bytes=0/0 timeout=43148/43200
  dec: spi=e89caf36 esp=aes key=16 26aa75c19207d423d14fd6fef2de3bcf
       ah=sha1 key=20 7d1a330af33fa914c45b80c1c96eafaf2d263ce7
  enc: spi=b721b907 esp=aes key=16 acb75d21c74eabc58f52ba96ee95587f
       ah=sha1 key=20 41120083d27eb1d3c5c5e464d0a36f27b78a0f5a
  dec:pkts/bytes=286338/40910978, enc:pkts/bytes=562327/62082855
  npu_flag=03 npu_rgwy=4.2.0.2 npu_lgwy=4.2.0.1 npu_selid=b dec_npuid=3 enc_npuid=1
```

Log into the CLI of any of the FIMs and run the command `diagnose test application fctrlproxyd 2`. The output should show matching destination subnets.

```
diagnose test application fctrlproxyd 2

fcp route dump : last_update_time 24107

Slot:4
       routecache entry: (5)
       checksum:27 AE 00 EA 10 8D 22 0C D6 48 AB 2E 7E 83 9D 24
       vd:3 p1:to-fgt2 p2:to-fgt2 subnet:4.2.3.0 mask:255.255.255.0 enable:1
       vd:3 p1:to-fgt2 p2:to-fgt2 subnet:4.2.4.0 mask:255.255.255.0 enable:1
```

```
vd:3 p1:to-fgt2 p2:to-fgt2 subnet:4.2.5.0 mask:255.255.255.0 enable:1
==========================================
```

FortiGate-7000 high availability

FortiGate-7000 for FortiOS 6.0 supports the following types of HA operation:

- FortiGate Clustering protocol (FGCP)
- FortiGates Session Life Support Protocol (FGSP) (FortiGate-7000 FGSP HA on page 95)
- Virtual Router Redundancy Protocol (VRRP) (FortiGate-7000 VRRP HA on page 99)

New HA features and changes

FortiGate Session Life Support Protocol (FGSP) (also called standalone session sync) is supported. See FortiGate-7000 FGSP HA on page 95.

FGSP session synchronization changes

The following session synchronization options apply to 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
```

- Turning on session synchronization for TCP sessions by enabling `session-pickup` also turns on session synchronization for connectionless protocol sessions, such as ICMP and UDP, by enabling `session-pickup-connectionless`. You can choose to reduce processing overhead by not synchronizing connectionless sessions if you don't need to.
- 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 does not currently work for IPv6 TCP traffic. This known issue (553996) will be fixed in a future firmware version.
- 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).

Introduction to FortiGate-7000 FGCP HA

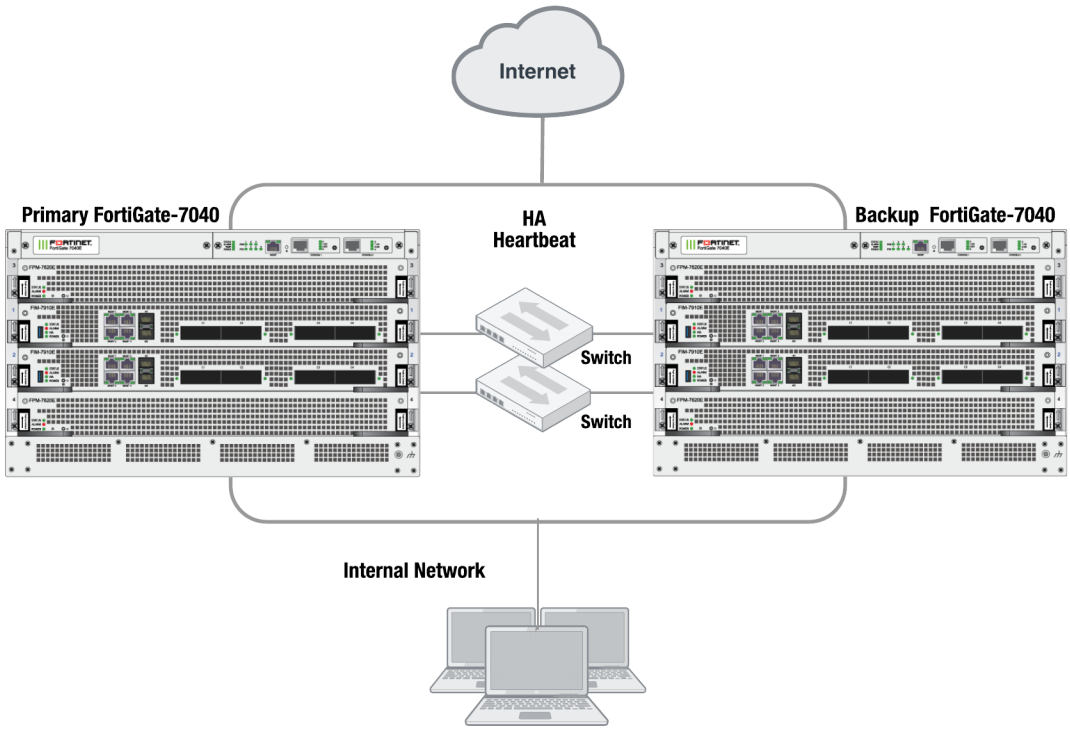
FortiGate-7000 supports active-passive FortiGate Clustering Protocol (FGCP) HA between two (and only two) identical FortiGate-7000s. You can configure FortiGate-7000 HA in much the same way as any FortiGate HA setup except that

only active-passive HA is supported, and even though FortiGate-7000s are configured with VDOMS, virtual clustering is not supported.

You must use the 10Gbit M1 and M2 interfaces for HA heartbeat communication. See Connect the M1 and M2 interfaces for HA heartbeat communication on page 73. Heartbeat packets are VLAN-tagged and you can configure the VLANs used. You must configure the switch interfaces used to connect the M1 and M2 interfaces in trunk mode and the switches must allow the VLAN-tagged packets.

As part of the FortiGate-7000 HA configuration, you assign each of the FortiGate-7000s in the HA cluster a chassis ID of 1 or 2. The chassis IDs just allow you to identify individual FortiGate-7000s and do not influence primary unit selection.

Example FortiGate-7040 HA configuration



In a FortiGate-7000 FGCP HA configuration, the primary (or master) FortiGate-7000 processes all traffic. The backup FortiGate-7000 operates in hot standby mode. The FGCP synchronizes the configuration, active sessions, routing information, and so on to the backup FortiGate-7000. If the primary FortiGate-7000 fails, traffic automatically fails over to the backup.

The FGCP selects the primary FortiGate-7000 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-7000 with the highest serial number becomes the primary FortiGate-7000. You can set the device priority higher on one of the

FortiGate-7000s if you want it to become the primary FortiGate-7000. You can also enable override along with setting a higher device priority to make sure the same FortiGate-7000 always becomes the primary FortiGate-7000.

Before you begin configuring HA

Before you begin:

- The FortiGate-7000s 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-7000 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-7000s 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.

Configure split ports

If required, you should configure split ports on the FIMs on both FortiGate-7000s before configuring HA because the FortiGate-7000 has to reboot to enable the split port configuration.

For example, to split the C1, C2, and C4 interfaces of an FIM-7910E in slot 1, enter the following command:

```
config system global
     set split-port 1-C1 2-C1 2-C4
end
```

After configuring split ports, the FortiGate-7000 reboots and synchronizes the configuration.

On each FortiGate-7000, make sure configurations of the FIMs and FPMs are synchronized before starting to configure HA. You can use the following command to verify the synchronization status of all modules:

```
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
all: c0 68 d2 67 e1 23 d9 3a 10 50 45 c5 50 f1 e6 8e
```

If the FIMs and FPMs are synchronized, the checksums displayed should all be the same.

You can also use the following command to list the FIMs and FPMs that are synchronized. The example output shows all four modules in a FortiGate-7040E have been configured for HA and added to the cluster.

```
diagnose sys confsync status | grep in_sync
FIM10E3E16000062, Slave, uptime=58852.50, priority=2, slot_id=2:2, idx=3, flag=0x10, in_sync=1
FIM04E3E16000010, Slave, uptime=58726.83, priority=3, slot_id=1:1, idx=0, flag=0x10, in_sync=1
FIM04E3E16000014, Master, uptime=58895.30, priority=1, slot_id=2:1, idx=1, flag=0x10, in_sync=1
FIM10E3E16000040, Slave, uptime=58857.80, priority=4, slot_id=1:2, idx=2, flag=0x10, in_sync=1
FPM20E3E16900234, Slave, uptime=58895.00, priority=16, slot_id=2:3, idx=4, flag=0x64, in_sync=1
FPM20E3E16900269, Slave, uptime=58333.37, priority=120, slot_id=2:4, idx=5, flag=0x64, in_sync=1
```

```
FPM20E3E17900113, Slave, uptime=58858.90, priority=116, slot_id=1:3, idx=6, flag=0x64, in_sync=1
FPM20E3E17900217, Slave, uptime=58858.93, priority=117, slot_id=1:4, idx=7, flag=0x64, in_sync=1
...
```

In this command output, `in_sync=1` means the module is synchronized with the primary FIM and `in_sync=0` means the module is not synchronized.

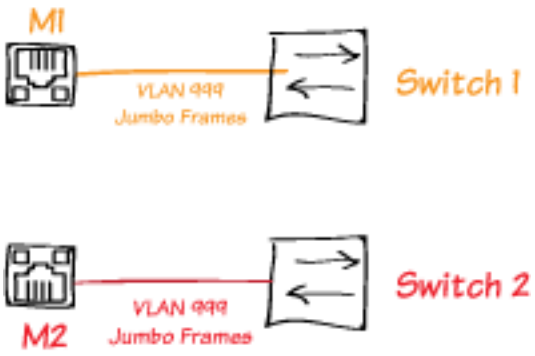
Connect the M1 and M2 interfaces for HA heartbeat communication

HA heartbeat communication between FortiGate-7000s happens over the 10Gbit M1 and M2 interfaces of the FIMs in each chassis. To set up HA heartbeat connections:

- Connect the M1 interfaces of all FIMs together using a switch.
- Connect the M2 interfaces of all FIMs together using another switch.

All of the M1 interfaces must be connected together with a switch and all of the M2 interfaces must be connected together with another switch. Connecting M1 interfaces or M2 interfaces directly is not supported as each FIM needs to communicate with all other FIMs. Because the FortiGate-7030E only has one FIM, in a FortiGate-7030E HA cluster you can directly connect the M1 and M2 interfaces of each FortiGate-7030E together, without using a switch.

Connect the M1 and M2 interfaces before enabling HA. Enabling HA moves heartbeat communication between the FIMs in the same chassis to the M1 and M2 interfaces. So if these interfaces are not connected before you enable HA, FIMs in the same chassis will not be able to communicate with each other.



Heartbeat packets are VLAN packets with VLAN ID 999 and ethertype 9890. The MTU value for the M1 and M2 interfaces is 1500.

You can use the following command to change the HA heartbeat packet VLAN ID and ethertype values if required for your switches. By default the M1 and M2 interface heartbeat packets use the same VLAN IDs. The following example changes the M1 VLAN ID to 4086 and the M2 VLAN ID to 4087.

```
config system ha
   set hbdev "1-M1" 50 "2-M1" 50 "1-M2" 50 "2-M2" 50
   set hbdev-vlan-id 4086
   set hbdev-second-vlan-id 4087
   set ha-eth-type <eth-type>
end
```

For this configuration to work, you must change both VLAN IDs. You cannot use the default value of 999.

Recommended HA heartbeat interface configuration

If you are setting up an HA configuration of two FortiGate-7030Es installed in the same location, you can directly connect their M1 interfaces and their M2 interfaces without using switches.

For redundancy, for other FortiGate-7000s, Fortinet recommends using separate switches for the M1 and M2 connections.These switches should be dedicated to HA heartbeat communication and not used for other traffic.

If you use the same switch for the M1 and M2 interfaces, separate the M1 and M2 traffic on the switch and set the heartbeat traffic on the M1 and M2 interfaces to have different VLAN IDs.

Example FortiGate-7000 switch configuration

The switch that you use for connecting HA heartbeat interfaces 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-7030E HA configurations if you have set up direct connections between the HA heartbeat interfaces.

This example shows how to configure a FortiGate-7000 to use different VLAN IDs for the M1 and M2 HA heartbeat interfaces and then how to configure two ports 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-7000s in the HA configuration, enter the following command to use different VLAN IDs for the M1 and M2 interfaces. The command sets the M1 VLAN ID to 4086 and the M2 VLAN ID to 4087:

```
config system ha
   set hbdev "1-M1" 50 "2-M1" 50 "1-M2" 50 "2-M2" 50
   set hbdev-vlan-id 4086
   set hbdev-second-vlan-id 4087
end
```

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

```
get system ha status
...
HBDEV stats:
 FG74E83E16000015(updated 1 seconds ago):
   1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=579602089/2290683/0/0,
tx=215982465/761929/0/0, vlan-id=4086
   2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=577890866/2285570/0/0,
tx=215966839/761871/0/0, vlan-id=4086
   1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=579601846/2290682/0/0,
tx=215982465/761929/0/0, vlan-id=4087
   2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=577890651/2285569/0/0,
tx=215966811/761871/0/0, vlan-id=4087
 FG74E83E16000016(updated 1 seconds ago):
```

```
   1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=598602425/2290687/0/0,
tx=196974887/761899/0/0, vlan-id=4086
   2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=596895956/2285588/0/0,
tx=196965052/761864/0/0, vlan-id=4086
   1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=598602154/2290686/0/0,
tx=196974915/761899/0/0, vlan-id=4087
   2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=596895685/2285587/0/0,
tx=196965080/761864/0/0, vlan-id=4087
...
```

3. Configure the Cisco switch port that connects the M1 interfaces to allow packets with a VLAN ID of 4086:

```
interface <name>
switchport mode trunk
switchport trunk native vlan 777
switchport trunk allowed vlan 4086
```

4. Configure the Cisco switch port that connects the M2 interfaces to allow packets with a VLAN ID of 4087:

```
interface <name>
switchport mode trunk
switchport trunk native vlan 777
switchport trunk allowed vlan 4087
```

Basic FortiGate-7000 HA configuration

Use the following steps to set up HA between two FortiGate-7000s. To configure HA, you assign a chassis ID (1 and 2) to each of the FortiGate-7000s. These IDs allow the FGCP to identify the chassis and do not influence primary FortiGate selection. Before you start, determine which FortiGate-7000 should be chassis 1 and which should be chassis 2.

1. Set up HA heartbeat communication as described in Connect the M1 and M2 interfaces for HA heartbeat communication on page 73.
2. Log into the GUI or CLI of the FIM in slot 1 of the FortiGate-7000 that will become chassis 1.
   Usually you would do this by connecting the management IP address of this FortiGate-7000.
3. Use the following CLI command to change the host name. This step is optional, but setting a host name makes the FortiGate-7000 easier to identify after the cluster has formed.

```
config system global
   set hostname 7K-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-7000:

```
config system ha
   set group-id <id>
   set group-name My-7K-Cluster
   set mode a-p
   set hbdev 1-M1 50 1-M2 50 2-M1 50 2-M2 50
   set chassis-id 1
   set hbdev-vlan-id 4086
   set hbdev-second-vlan-id 4087
   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 (1-M1, 1-M2, 2-M1, and 2-M2). You must configure the chassis ID and group ID from the CLI.

5. Log into the chassis 2 FortiGate-7000 and configure its host name, for example:

```
config system global
   set hostname 7K-Chassis-2
end
```

From the GUI you can configure the host name by going to **System > Settings** and changing the **Host name**.

6. 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 <id>
   set group-name My-7K-Cluster
   set mode a-p
   set hbdev 1-M1 50 1-M2 50 2-M1 50 2-M2 50
   set chassis-id 2
   set hbdev-vlan-id 4086
   set hbdev-second-vlan-id 4087
   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 (1-M1, 1-M2, 2-M1, and 2-M2). You must configure the chassis ID and group ID from the CLI.

Once you save your configuration changes, if the HA heartbeat interfaces are connected, the FortiGate-7000s negotiate to establish a cluster. You may temporarily lose connectivity with the FortiGate-7000s as the cluster negotiates and the FGCP changes the MAC addresses of the FortiGate-7000 interfaces. .

7. 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 M1 and M2 interfaces for HA heartbeat communication on page 73.

You should also review the HA configurations of the FortiGate-7000s. When checking the configurations, make sure both FortiGate-7000s have the same HA configuration, including identical HA group IDs, group names, passwords, and HA heartbeat VLAN IDs.

The following example FortiGate-7000 `get system ha status` output shows a FortiGate-7000 cluster that is operating normally. The output shows which FortiGate-7000 has become the primary (master) FortiGate-7000 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-7000E
```

```
Mode: HA A-P
Group: 7
Debug: 0
Cluster Uptime: 0 days 16:42:5
Cluster state change time: 2019-01-14 16:26:30
    <2019/01/14 16:26:30> FG74E83E16000016 is selected as the master because it has more act-
ive switch blade.
    <2019/01/14 16:26:12> FG74E83E16000016 is selected as the master because it's the only mem-
ber in the cluster.
ses_pickup: disable
override: disable
Configuration Status:
    FG74E83E16000016(updated 4 seconds ago): in-sync
    FG74E83E16000015(updated 0 seconds ago): in-sync
System Usage stats:
    FG74E83E16000016(updated 4 seconds ago):
        sessions=198, average-cpu-user/nice/system/idle=1%/0%/0%/97%, memory=5%
    FG74E83E16000015(updated 0 seconds ago):
        sessions=0, average-cpu-user/nice/system/idle=2%/0%/0%/96%, memory=6%
HBDEV stats:
    FG74E83E16000016(updated 4 seconds ago):
        1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=227791977/902055/0/0,
tx=85589814/300318/0/0, vlan-id=4086
        2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=227119632/900048/0/0,
tx=85589814/300318/0/0, vlan-id=4086
        1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=227791977/902055/0/0,
tx=85589814/300318/0/0, vlan-id=4087
        2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=227119632/900048/0/0,
tx=85589814/300318/0/0, vlan-id=4087
    FG74E83E16000015(updated 0 seconds ago):
        1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=0/0/0/0,
tx=85067/331/0/0, vlan-id=4086
        2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=947346/3022/0/0,
tx=206768/804/0/0, vlan-id=4086
        1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=0/0/0/0,
tx=85067/331/0/0, vlan-id=4087
        2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=946804/3020/0/0,
tx=206768/804/0/0, vlan-id=4087
Master: 7K-Chassis-1    , FG74E83E16000016, cluster index = 0
Slave : 7K-Chassis-2    , FG74E83E16000015, cluster index = 1
number of vcluster: 1
vcluster 1: work 10.101.11.20
Master: FG74E83E16000016, operating cluster index = 0
Slave : FG74E83E16000015, 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
```

Setting up HA management connections

Fortinet recommends the following configurations for redundant management connections to a FortiGate-7000 HA configuration.

- Single management connections to each of the FIMs.
- Redundant management connections to each of the FIMs.

These management connections involve connecting the static redundant management interfaces (MGMT1 to MGMT4) of each FIM in the HA configuration to one or more switches. You do not have to change the FortiGate-7000 configuration to set up redundant management connections. However, specific switch configurations are required for each of these configurations as described below.

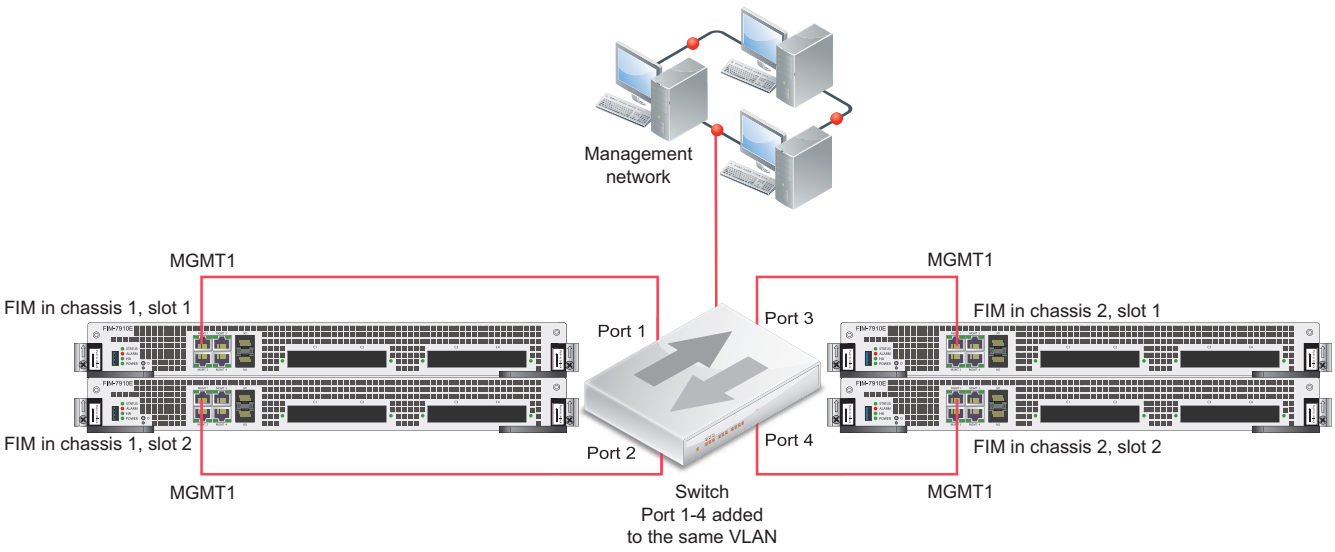
LACP is not supported for the mgmt aggregate interface.

Setting up single management connections to each of the FIMs

The simplest way to provide redundant management connections to a FortiGate-7000 HA configuration involves connecting the MGMT1 interface of each of the FIMs to four ports on a switch. On the switch you must add the four switch ports to the same VLAN. Then connect the switch to your management network and allow traffic from the VLAN to the management network.

A FortiGate-7030E HA configuration only has two FIMs so would only require two switch ports.

Example FortiGate-7000 HA redundant management connections



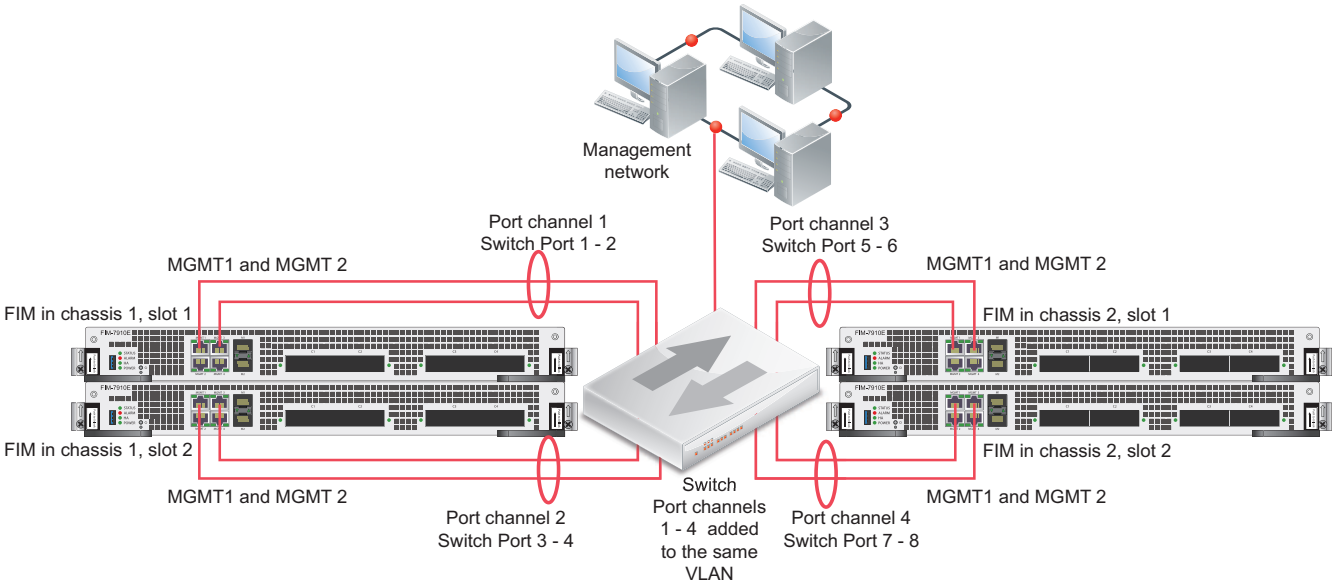
Setting up redundant management connections to each of the FIMs

You can enhance redundancy by setting up two redundant management connections to each FIM. To support this configuration, on the switch you must create a port channel for each FIM interface. Create a total of four port channels, one for each FIM and add each of the port channels to the same VLAN. Then connect the switch to your management network and allow traffic from the VLAN to the management network.

If you use two switches, the VLAN should span across both switches.

A FortiGate-7030E HA configuration only has two FIMs so would only require two port channels.

Example FortiGate-7000 HA redundant management connections with redundant connections to each FIM



Managing individual modules in HA mode

In some cases you may want to connect to an individual FIM or FPM in a specific FortiGate-7000. For example, you may want to view the traffic being processed by the FPM in slot 3 of the FortiGate-7000 designated as chassis 2. You can connect to the GUI or CLI of individual modules in the chassis using the system management IP address with a special port number.

For example, if the system management IP address is 1.1.1.1 you can browse to https://1.1.1.1:44323 to connect to the FPM in the FortiGate-7000 chassis 2 slot 3. The special port number (in this case 44323) is a combination of the service port, chassis ID, and slot number. The following table lists the special ports for common admin protocols:

FortiGate-7000 HA special administration port numbers

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch1 slot 5	FPM05	8005	44305	2305	2205	16105
Ch1 slot 3	FPM03	8005	44303	2303	2203	16103
Ch1 slot 1	FIM01	8003	44301	2301	2201	16101
Ch1 slot 2	FIM02	8002	44302	2302	2202	16102
Ch1 slot 4	FPM04	8004	44304	2304	2204	16104
Ch1 slot 6	FPM06	8006	44306	2306	2206	16106
Ch2 slot 5	FPM05	8005	44325	2325	2225	16125
Ch2 slot 3	FPM03	8005	44323	2323	2223	16123
Ch2 slot 1	FIM01	8003	44321	2321	2221	16121
Ch2 slot 2	FIM02	8002	44322	2322	2222	16122
Ch2 slot 4	FPM04	8004	44324	2324	2224	16124
Ch2 slot 6	FPM06	8006	44326	2326	2226	16126

HA cluster firmware upgrades

All of the FIMs and FPMs in a FortiGate-7000 HA cluster run the same firmware image. You upgrade the firmware from the primary FIM in the primary FortiGate-7000 .

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-7000 primary FIM uploads firmware to the backup FortiGate-7000 primary FIM, which uploads the firmware to all of the modules in the backup FortiGate-7000. Then the modules in the backup FortiGate-7000 upgrade their firmware, reboot, and resynchronize.

Then all traffic fails over to the backup FortiGate-7000 which becomes the new primary FortiGate-7000. Then the modules in the new backup FortiGate-7000 upgrade their firmware and rejoin the cluster. Unless override is enabled, the new primary FortiGate-7000 continues to operate as the primary FortiGate-7000.

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 DP2 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-7000 HA supports separating the FortiGate-7000s in an HA cluster to different physical locations. Distributed FortiGate-7000 HA clustering (or geographically distributed FortiGate-7000 HA or geo clustering) can involve two FortiGate-7000s 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.

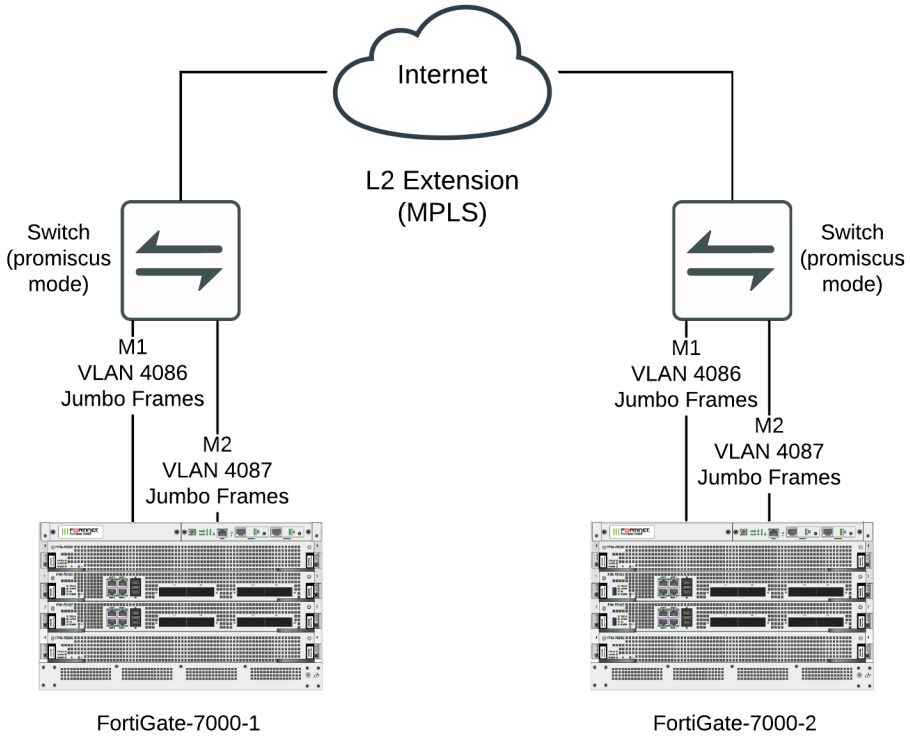
Just like any FortiGate-7000 HA configuration, distributed FortiGate-7000 HA requires heartbeat communication between the FortiGate-7000s over the M1 and M2 interfaces. In a distributed FortiGate-7000 HA configuration this heartbeat communication can take place over the Internet or over other transmission 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 M1 and M2 interface traffic must be separated. You can do this by using separate channels for each interface or by configuring the M1 and M2 interfaces to use different VLANs.

Example FortiGate-7000 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-7000s. 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 82.

Modifying heartbeat timing

If the FortiGate-7000s in the HA cluster do not receive heartbeat packets on time, the FortiGate-7000s in the HA configuration may each determine that the other FortiGate-7000 has failed. HA heartbeat packets may not be sent on time because of network issues. For example, if the M1 and M2 communications links between the FortiGate-7000s become too busy to handle the heartbeat traffic. Also, in a distributed clustering configuration the round trip time (RTT) between the FortiGate-7000s may be longer the expected time between heartbeat packets.

In addition, if the FortiGate-7000s becomes excessively busy, they may delay sending heartbeat packets.

Even with these delays, the FortiGate-7000 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 does not receive before assuming that a failure has occurred. The default value of 6mean that if a FortiGate-7000 does not receive 6 heartbeat packets it determines that the other FortiGate-7000 in the cluster has failed. The range is 1 to 60 packets.

The lower the `hb-lost-threshold`, the faster a FortiGate-7000 HA configuration responds when a failure occurs. However, sometimes heartbeat packets may not be received because the other FortiGate-7000 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-7000 waits before assuming that the other FortiGate-7000 has failed and is no longer sending heartbeat packets. By default, if a FortiGate-7000 does not receive a heartbeat packet from a cluster unit for 6 * 200 = 1200 milliseconds or 1.2 seconds the FortiGate-7000 assumes that the other FortiGate-7000 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-7000 waits before changing from hello state to work state. After a failure or when starting up, FortiGate-7000s in HA mode operate in the hello state to send and receive heartbeat packets to find each other and form a cluster. A FortiGate-7000 should change from the hello state to work state after it finds the FortiGate-7000 to form a cluster with. If for some reason the FortiGate-7000s cannot find each other during the hello state both FortiGate-7000s may assume that the other one has failed and each could form separate clusters of one FortiGate-7000. The FortiGate-7000s 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-7000s finding each other could be the FortiGate-7000s are located at different sites or for some other reason communication is delayed between the heartbeat interfaces. If you find that your FortiGate-7000s 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, communications sessions resume on the new primary FortiGate-7000 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

Session failover (also called session-pickup) is not enabled by default for FortiGate-7000 HA. If sessions pickup is enabled, while the FortiGate-7000 HA cluster is operating the primary FortiGate-7000 informs the backup FortiGate-7000 of changes to the primary FortiGate-7000 connection and state tables for TCP and UDP sessions passing through the cluster, keeping the backup FortiGate-7000 up-to-date with the traffic currently being processed by the cluster.

After a failover the new primary FortiGate-7000 recognizes open sessions that were being handled by the cluster. The sessions continue to be processed by the new primary FortiGate-7000 and are handled according to their last known state.

Session-pickup has some limitations. For example, session failover is not supported 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 VPN, 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 synchronization 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-7000 TCP and connectionless session tables are synchronized to the backup FortiGate-7000. As soon as a new session is added to the primary FortiGate-7000 session table, that session is synchronized to the backup FortiGate-7000. This synchronization happens as quickly as possible to keep the session tables synchronized.

If the primary FortiGate-7000 fails, the new primary FortiGate-7000 uses its synchronized session tables to resume all TCP and connectionless sessions that were being processed by the former primary FortiGate-7000 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-7000 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-7000 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
```

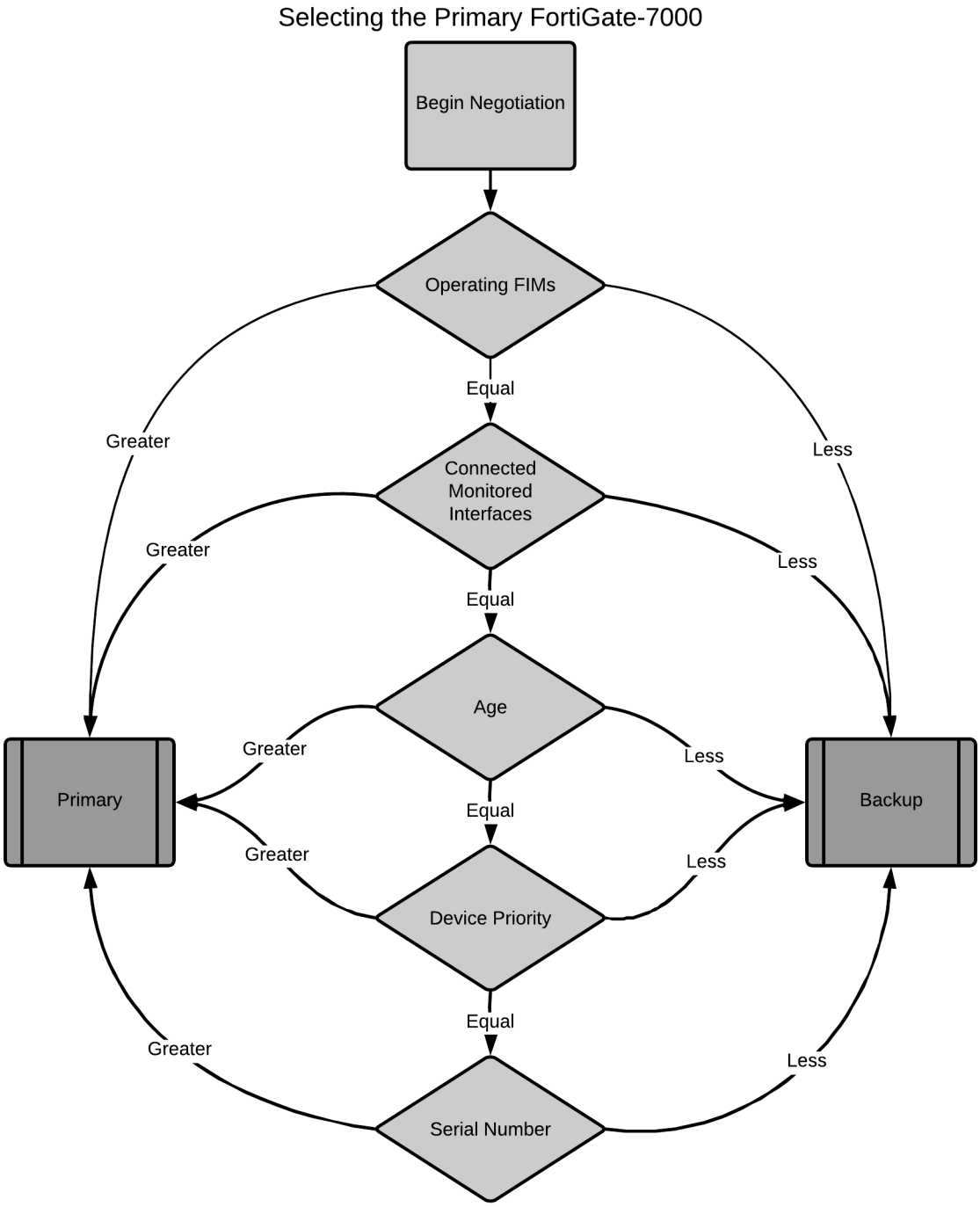
Enabling session pickup delay means that if a failover occurs more TCP sessions may not be resumed after a failover. In most cases short duration sessions can be restarted with only a minor traffic interruption. However, if you notice too many sessions not resuming after a failover you might want to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

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

Primary FortiGate-7000 selection

Once two FortiGate-7000s recognize that they can form a cluster, they negotiate to select a primary FortiGate-7000. Primary FortiGate-7000 selection occurs automatically based on the selection criteria shown in the diagram below. After the cluster selects the primary FortiGate-7000, the other FortiGate-7000 becomes the backup.

Negotiation and primary FortiGate-7000 selection also takes place if the one of the criteria for selecting the primary FortiGate-7000 changes. For example, an interface can become disconnected or an FIM can fail. After this happens, the cluster can renegotiate to select a new primary FortiGate-7000 using the same selection criteria.



If there are no FIM failures and if you haven't configured any settings to influence primary FortiGate-7000 selection, the FortiGate-7000 with the highest serial number becomes the primary FortiGate-7000.

This section highlights some aspects of primary FortiGate-7000 selection. For more details about how this works, see Primary unit selection.

Age and primary FortiGate-7000 selection

Age (or uptime) is also a factor in primary FortiGate-7000 selection. Normally when two FortiGate-7000s start, their uptimes are similar and do not affect primary FortiGate-7000 selection. However, during operation, if one of the FortiGate-7000s goes down the other will have a much higher age or uptime and will be selected as the primary FortiGate-7000 before checking priority and serial number.

In some cases, age differences can result in the wrong FortiGate-7000 becoming the primary FortiGate-7000. For example, if the FortiGate-7000 set to a high priority reboots, it will have a lower age than other FortiGate-7000 when it rejoins the cluster. Since age takes precedence over priority it will become the backup FortiGate-7000 when it rejoins the cluster.

One way to resolve this issue is to reboot both FortiGate-7000s in the cluster at the same time to reset the age of both FortiGate-7000s. However, doing this would disrupt traffic. Instead you can use the following command to reset the age of one the primary FortiGate-7000 to zero.

```
diagnose sys ha reset-uptime
```

The primary FortiGate-7000 now has the lowest age and the other FortiGate-7000 will have the highest age and can then become the primary FortiGate-7000.

The `diagnose sys ha reset-uptime` command should only be used as a temporary solution. You should reboot the FortiGate-7000s during a maintenance window to permanently bring their ages back together.

Device priority and primary FortiGate-7000 selection

In some situations you may want to select a FortiGate-7000 to always become the primary FortiGate-7000. You can do this by setting its device priority higher. You can change the device priority of an FIM from the **System > HA** GUI page or by using the following command:

```
config system ha
   set priority <number>
end
```

The default priority is 128.

During negotiation, the FortiGate-7000 with the highest device priority becomes the primary FortiGate-7000.

Override and primary FortiGate-7000 selection

You can enable override to select a FortiGate-7000 to always becomes the primary FortiGate-7000. Enabling override changes how primary select works. For details, see Override and primary FortiGate-7000 selection on page 1.

FIM or FPM failure and primary FortiGate-7000 selection

If an FIM or an FPM fails, the FortiGate-7000 cluster negotiates to select a new Primary FortiGate-7000 and the FortiGate-7000 with the most operating FIMs becomes the primary FortiGate-7000.

You can also configure board failover tolerance to control how a FortiGate-7000 cluster responds to an FIM failure.

```
config system ha
   set board-failover-tolerance <tolerance>
end
```

Where <tollerance> can be from 0 to 3. A tolerance of 0 (the default) means that if a single FIM or FPM fails in the primary FortiGate-7000, a failover occurs and the FortiGate-7000 with the fewest failed modules becomes the new primary FortiGate-7000. Higher failover tolerances mean that more module failures must occur before an FGCP failover occurs.

Verifying primary FortiGate-7000 selection

You can use the get system ha status command to verify which FortiGate-7000 has become the primary FortiGate-7000. The command output shows which FortiGate-7000 is currently operating as the primary FortiGate-7000. The following command output excerpt shows that the FortiGate-7000 labeled as chassis 2 has become the primary (master) FortiGate-7000:

```
get system ha status
Master selected using:
HA Health Status: OK
Model: FortiGate-7000E
Mode: HA A-P
Group: 7
Debug: 0
Cluster Uptime: 0 days 16:42:5
...
Master: CH16            , FG74E83E16000016, cluster index = 0
Slave : FG74E83E16000015, FG74E83E16000015, cluster index = 1
number of vcluster: 1
vcluster 1: work 10.101.11.20
Master: FG74E83E16000016, operating cluster index = 0
Slave : FG74E83E16000015, 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
```

Primary FortiGate-7000 selection and override

When configuring FortiGate-7000 HA, if you want one of the FortGate-7000s to always become the primary FortiGate-7000 you can enable override on that FortiGate-7000. For override to be effective, you must also set the device priority highest on this FortiGate-7000.

To enable override and increase device priority:

```
config system ha
   set override enable
   set priority 200
end
```

The FortiGate-7000 with override enabled and the highest device priority always becomes the primary FortiGate-7000.

In most cases, with override enabled the cluster will negotiate more often. For example, with override enabled it is more likely that changes to the backup FortiGate-7000 may cause the cluster to negotiate. More frequent negotiation can lead to more traffic disruptions.

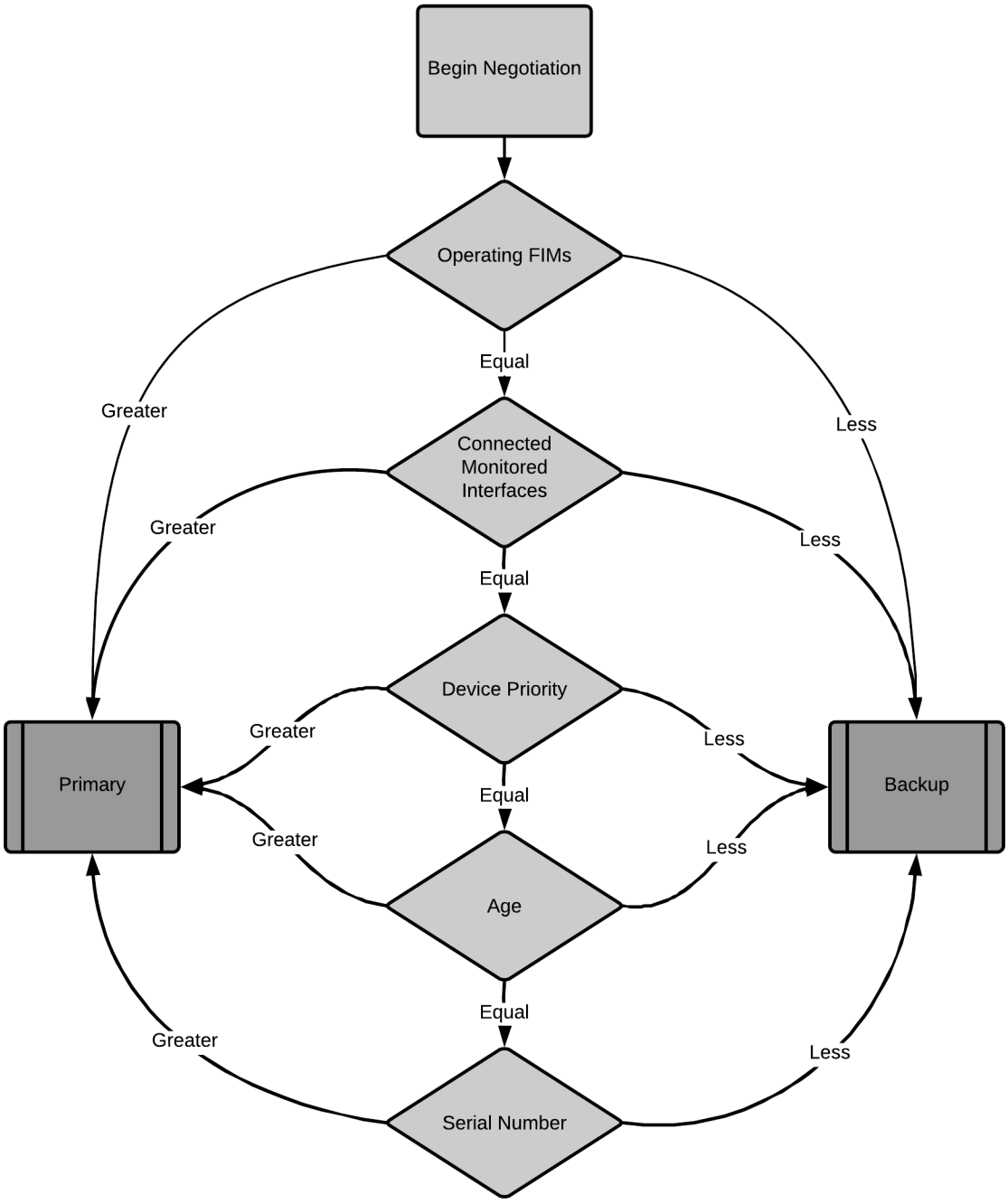
This section highlights some aspects of primary FortiGate-7000 selection. For more details about how this works, see HA override.

Enabling override changes primary FortiGate-7000 selection

Enabling `override` changes the order of primary FortiGate-7000 selection. As shown below, if `override` is enabled, primary FortiGate-7000 selection considers device priority before age and serial number. This means that if you set the device priority higher on one FortiGate-7000, with `override` enabled this FortiGate-7000 becomes the primary FortiGate-7000 even if its age and serial number are lower.

Similar to when `override` is disabled, when `override` is enabled primary FortiGate-7000 selection checks for operating FIMs and connected monitored interfaces first. So if interface monitoring is enabled, the FortiGate-7000 with the most disconnected monitored interfaces cannot become the primary FortiGate-7000, even if this FortiGate-7000 has the highest device priority.

Selecting the Primary FortiGate-7000 with Override enabled



Link failover (port monitoring or interface monitoring)

Link failover means that if a monitored interface fails, the FortiGate-7000 cluster reorganizes to reestablish a link to the network that the monitored interface was connected to and to continue operating with minimal or no disruption of network traffic.

You configure monitored interfaces (also called interface monitoring or port monitoring) by selecting FIM front panel interfaces to monitor as part of the HA configuration.

You can monitor up to 64 interfaces. The FGCP synchronizes the interface monitoring configurations to both FortiGate-7000s in the cluster.

The interfaces that you can monitor appear on the HA GUI page **Monitor Interfaces** list. You can monitor any FIM interfaces including redundant interfaces and 802.3ad aggregate interfaces.

You cannot monitor the following types of interfaces (you cannot select these types of interfaces on the Monitor Interfaces list):

- VLAN subinterfaces.
- IPsec VPN interfaces.
- Individual physical interfaces that have been added to a redundant or 802.3ad aggregate interface.

You should only monitor interfaces that are connected to networks, because a failover may occur if you monitor an unconnected interface. For this reason, you should also wait until your FortiGate-7000 HA setup has been configured and connected and is operating as expected before enabling interface monitoring.

To enable interface monitoring

From the GUI, go to **System > HA** and add interfaces to the **Monitor Interfaces** list.

From the CLI, enter the following command to monitor the 1-B1/2 and 2-C1/10 interfaces:

```
config system ha
   set monitor 1-B1/2 2-C1/10
end
```

With interface monitoring enabled, during FortiGate-7000 cluster operation, the cluster monitors each FIM in the cluster to determine if the monitored interfaces are operating and connected. Each FIM can detect a failure of its network interface hardware.

FIMs cannot determine if the switches that its interfaces are connected to are still connected to networks. However, you can use remote IP monitoring to make sure that the cluster unit can connect to downstream network devices. See Remote link failover on page 93.

If a monitored interface on the primary FortiGate-7000 fails

Because the primary FortiGate-7000 receives all traffic processed by the cluster, a FortiGate-7000 cluster can only process traffic from a network if the primary FortiGate-7000 can connect to it. So, if the link between a network and the

primary FortiGate-7000 fails, to maintain communication with this network, the cluster must set the FortiGate-7000 that is still connected to this network to become the primary FortiGate-7000. Unless another link failure has occurred, the new primary FortiGate-7000 will have an active link to the network and will be able to maintain communication with it.

To support link failover, the FortiGate-7000s store link state information for all monitored interfaces in a link state database. If one of the monitored interfaces on one of the FortiGate-7000s becomes disconnected or fails, this information is immediately shared with the other FortiGate-7000 in the cluster.

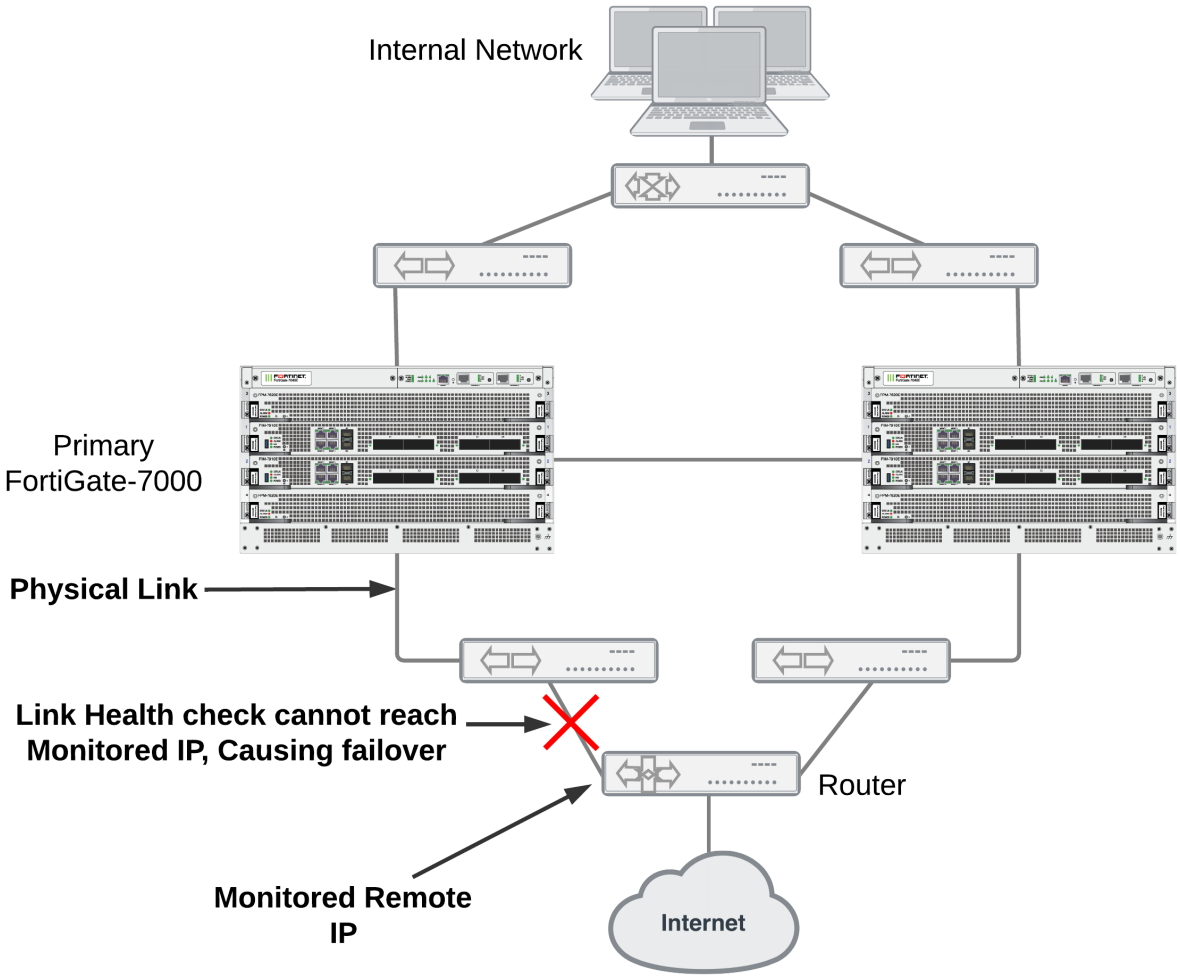
If a monitored interface on the primary FortGate-7000 fails, the cluster renegotiates to select the primary FortiGate-7000 using the process described in Primary FortiGate-7000 selection on page 86. Because the FortGate-7000 with the failed monitored interface has the lowest monitor priority, the other FortiGate-7000 becomes the primary FortiGate-7000. The new primary FortiGate-7000 should have fewer link failures.

If a monitored interface on the backup FortiGate-7000 fails

If a monitored interface on a the backup FortiGate-7000 fails, this information is shared with the primary FortiGate-7000. The cluster does not renegotiate. The backup FortiGate-7000 with the failed monitored interface continues to function in the cluster.

Remote link failover

Remote link failover (also called remote IP monitoring) is similar to interface monitoring and link health monitoring (also known as dead gateway detection). Remote IP monitoring uses link health monitors to test connectivity between the primary FortiGate-7000 and remote network devices such as a downstream router. Remote IP monitoring causes a failover if one or more of these remote IP addresses does not respond to link health checking.



In the simplified example topology shown above, the switch connected directly to the primary FortiGate-7000 is operating normally but the link on the other side of the switches fails. As a result, traffic can no longer flow between the primary ForitiGate-7000 and the Internet.

This section highlights some aspects of primary FortiGate-7000 remote link failover. For more details about how this works, see Remote link failover.

Configuring remote IP monitoring

Enter the following command to enable HA remote IP monitoring on the 1-B1/1 interface:

```
config system ha
   set pingserver-monitor-interface 1-B1/1
   set pingserver-failover-threshold 5
   set pingserver-flip-timeout 120
end
```

Keep the `pingserver-failover-threshold` set to the default value of 5. This means a failover occurs if the link health monitor doesn't get a response after 5 attempts.

Set the `pingserver-flip-timeout` set to 120 minutes. After a failover, if HA remote IP monitoring on the new primary unit also causes a failover, the flip timeout prevents the failover from occurring until the timer runs out. Setting the `pingserver-flip-timeout` to 120 means that remote IP monitoring can only cause a failover every 120 minutes. This flip timeout is required to prevent repeating failovers if remote IP monitoring causes a failover from all cluster units because none of the cluster units can connect to the monitored IP addresses.

Enter the following command to add a link health monitor for the 1-B1/1interface and to set HA remote IP monitoring priority for this link health monitor.

```
config system link-monitor
   edit ha-link-monitor
   set server 192.168.20.20
   set srcintf port2
   set ha-priority 1
   set interval 5
   set failtime 2
end
```

The `detectserver` option sets the remote IP address to monitor to 192.168.20.20.

Leave the `ha-priority` keyword set to the default value of 1. You only need to change this priority if you change the HA `pingserver-failover-threshold`. The `ha-priority` setting is not synchronized among the FortiGate-7000s in the HA configuration.

The `ha-priority` setting is not synchronized. So if you want to change the `ha-priority` setting you must change it separately on each FortiGate-7000. Otherwise it will remain set to the default value of 1.

Use the `interval` option to set the time between link health checks and use the `failtime` keyword to set the number of times that a health check can fail before a failure is detected (the failover threshold). The example reduces the failover threshold to 2 but keeps the health check interval at the default value of 5.

FortiGate-7000 FGSP HA

FortiGate-7000 supports the FortiGate Session Life Support Protocol (FGSP) (also called standalone session sync) HA to synchronize sessions among up to four FortiGate-7000s. All of the FortiGate-7000s 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-7000 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-7000 FGSP can use the 1-M1 and 1-M2 and 2-M1 and 2-M2 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-7000 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 57 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-7000 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-7000s 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 TCP sessions older than 30 seconds

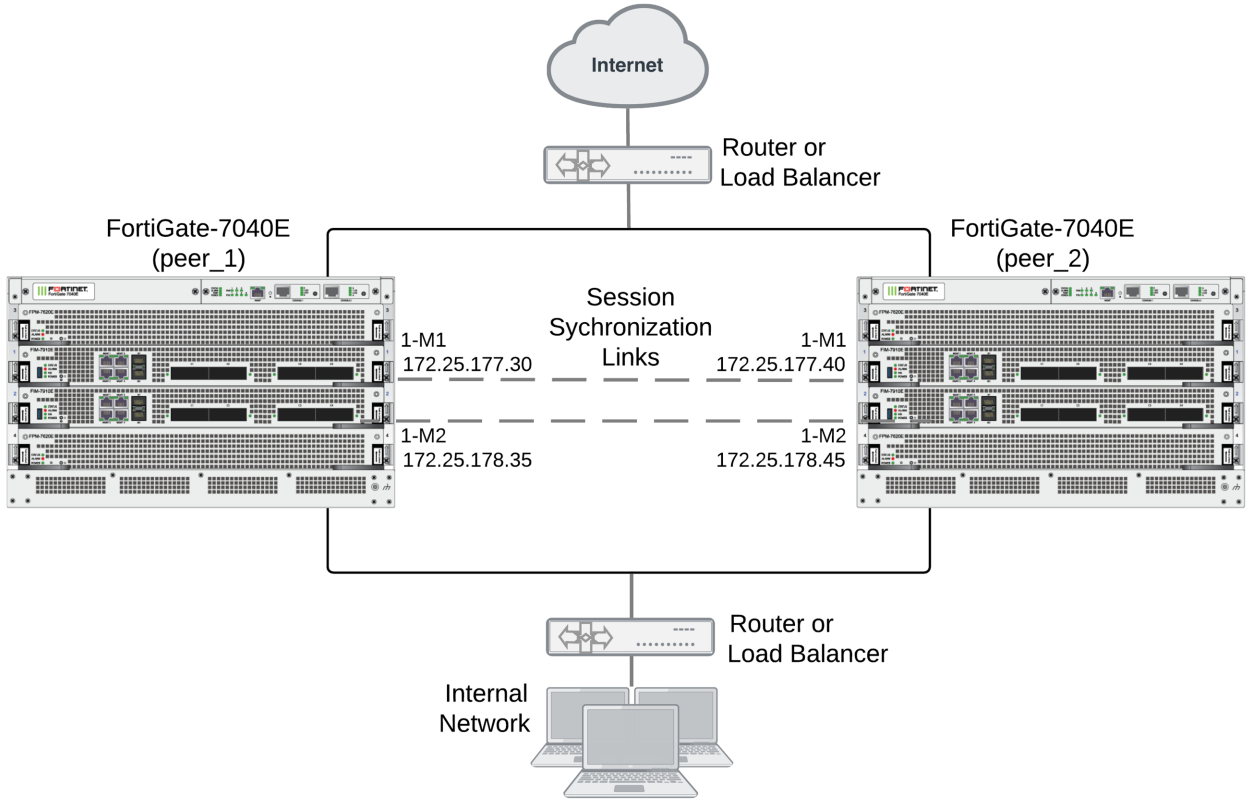
Enable `session-pickup-delay` to synchronize TCP sessions only if they remain active for more than 30 seconds. This option improves performance when `session-pickup` is enabled by reducing the number of sessions that are synchronized. This option does not affect SCTP or connectionless sessions.

Example FortiGate-7000 FGSP configuration

This example shows how to configure an FGSP cluster to synchronize sessions between two FortiGate-7040Es for two VDOMs: VDOM-1 and VDOM-2. The example uses the 1-M1 interface for VDOM-1 session synchronization and the 1-M2 interface for VDOM-2 session synchronization. The 1-M1 interfaces are connected to the 172.25.177.0/24 network and the 1-M2 interfaces are connected to the 172.25.178.0/24 network.

Because configuration synchronization is not supported for FGSP you must set up both FortiGate-7040Es with the same configuration, including the VDOMs to be synchronized and these VDOMs must have the same firewall policies. The two FortiGate-7040Es must have their own IP addresses and their own networking configuration. In addition, you can give the FortiGate--7040Es different host names to make them easier to identify.

Example FortiGate-7000 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-7040E a different host name (in this case peer_1 and peer_2).
4. Configure network settings for each FortiGate-7040E to allow them to connect to their networks and route traffic.
5. Add VDOM-1 and VDOM-2 to each FortiGate-7040E.
6. Configure VDOM-1 on each FortiGate-7040E with the same firewall policies.
7. Configure VDOM-2 on each FortiGate-7040E with the same firewall policies.
8. Configure the 1-M1 and 1-M2 interfaces of the peer_1 FortiGate-7040E with IP addresses on the 172.25.177.0/24 and 172.25.178.0/24 networks:

```
config system interface
   edit 1-M1
      set ip 172.25.177.30 255.255.255.0
   next
   edit 1-M2
      set ip 172.25.178.35 255.255.255.0
   end
```

9. Configure the 1-M1 and 1-M2 interfaces of the peer_2 FortiGate-7040E with IP addresses on the 172.25.177.0/24 and 172.25.178.0/24 networks:

```
config system interface
   edit 1-M1
      set ip 172.25.177.40 255.255.255.0
```

```
   next
   edit 1-M2
      set ip 172.25.178.45 255.255.255.0
   end
```

10. On the peer_1 FortiGate-7040E, configure session synchronization for VDOM-1 and VDOM-2.

```
config system cluster-sync
   edit 1
      set peervd mgmt-vdom
      set peerip 172.25.177.40
      set syncvd VDOM-1
   next
   edit 2
      set peervd mgmt-vdom
      set peerip 172.25.178.45
      set syncvd VDOM-2
   next
```

For VDOM-1, `peervd` will always be `mgmt-vdom`, the `peerip` is the IP address of the 1-M1 interface of the peer_2 FortiGate-7040E, and `syncvd` is VDOM-1.

For VDOM-2, `peervd` will always be `mgmt-vdom`, the `peerip` is the IP address of the 1-M2 interface of the peer_2 FortiGate-7040E, and `syncvd` is VDOM-2.

11. On the peer_2 FortiGate-7040E, configure session synchronization for VDOM-1 and VDOM-2.

```
config system cluster-sync
   edit 1
      set peervd mgmt-vdom
      set peerip 172.25.177.30
      set syncvd VDOM-1
   next
   edit 2
      set peervd mgmt-vdom
      set peerip 172.25.178.35
      set syncvd VDOM-2
   next
```

For VDOM-1, `peervd` will always be `mgmt-vdom`, the `peerip` is the IP address of the 1-M1 interface of the peer_1 FortiGate-7040E, and `syncvd` is VDOM-1.

For VDOM-2, `peervd` will always be `mgmt-vdom`, the `peerip` is the IP address of the 1-M2 interface of the peer_1 FortiGate-7040E, and `syncvd` is VDOM-2.

FortiGate-7000 VRRP HA

The FortiGate-7000 platform supports the Virtual Router Redundancy Protocol (VRRP), allowing you to configure VRRP HA between FortiGate-7000 devices. You can also add a FortiGate-7000 to a VRRP group with other VRRP routers.

Configure VRRP on the FortiGate-7000 by creating a VRRP group and adding one or more front panel interfaces to the group.

During normal operation, the primary FortiGate-7000 sends outgoing VRRP routing advertisements. Both the primary and backup FortiGate-7000s listen for incoming VRRP advertisements from other routers in the VRRP group. If the primary FortiGate-7000 fails, the new primary FortiGate-7000 takes over the role of both sending and receiving VRRP advertisements, maintaining the FortiGate-7000 within the VRRP group.

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

ICAP support

You can configure your FortiGate-7000 to use Internet Content Adaptation Protocol (ICAP) to offload processing that would normally take place on the FortiGate-7000 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-7000 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-7000 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 "1-C1/5"
      set dstintf "1-C1/6"
      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 "1-C1/7"
      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 FPM CLI to verify the mirrored traffic:

```
diagnose sniffer packet 1-C1/7 'port 443' -c 50
interfaces=[1-C1/7]
filters=[port 443]
pcap_lookupnet: 1-C1/7: 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-7000 v6.0.4 special features and limitations

This section describes special features and limitations for FortiGate-7000 v6.0.4.

Managing the FortiGate-7000

Management is only possible through the MGMT1 to MGMT4 front panel management interfaces. By default the MGMT1 to MGMT4 interfaces of the FIMs in slot 1 and slot 2 are in a single static aggregate interface named mgmt with IP address 192.168.1.99. You manage the FortiGate-7000 by connecting any one of these eight interfaces to your network, opening a web browser and browsing to the management IP address. For a factory default configuration, browse to https://192.168.1.99.

The FortiGate-7030E has one FIM and the MGMT1 to MGMT4 interfaces of that module are the only interfaces in the aggregate interface.

Default management VDOM

By default the FortiGate-7000 configuration includes a management VDOM named mgmt-vdom. For the FortiGate-7000 system to operate normally you should not change the configuration of this VDOM and this VDOM should always be the management VDOM. You should also not add or remove interfaces from this VDOM.

You have full control over the configurations of other FortiGate-7000 VDOMs.

Default Security Fabric configuration

The FortiGate-7000 uses the Security Fabric for communication and synchronization among FIMs and FPMs. 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-7000 to operate normally, you must not change the Security Fabric configuration.

Maximum number of LAGs

FortiGate-7000 systems support up to 16 link aggregation groups (LAGs). This includes both normal link aggregation groups and redundant interfaces and including the redundant interface that contains the mgmt1 to mgmt4 management interfaces.

Firewall

TCP sessions with NAT enabled that are expected to be idle for more than the distributed processing normal TCP timer (which is 3605 seconds) should only be distributed to the master FPM using a flow rule. You can configure the distributed normal TCP timer using the following command:

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

UDP sessions with NAT enabled that are expected to be idle for more than the distributed processing normal UDP timer should only be distributed to the primary FPM using a flow rule.

IP multicast

IPv4 and IPv6 Multicast traffic is only sent to the primary FPM (usually the FPM in slot 3). 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 M1 and M2 interfaces are used for the HA heartbeat communication. For information on how to set up HA heartbeat communication using the M1 and M2 interfaces, see Connect the M1 and M2 interfaces for HA heartbeat communication on page 73

The following FortiOS HA features are not supported or are supported differently by FortiGate-7000 v6.0.4:

- Active-active HA is not supported.
- The range for the HA `group-id` is 0 to 31.
- Failover logic for FortiGate-7000 HA is not the same as FGCP for other FortiGate clusters.
- HA heartbeat configuration is specific to FortiGate-7000 systems and differs from standard HA.
- FortiGate Session Life Support Protocol (FGSP) HA (also called standalone session synchronization) is not supported.
- FortiGate-7000 HA does not support the `route-ttl`, `route-wait`, and `route-hold` options for tuning route synchronization between FortiGate-7000s.

Shelf manager module

It is not possible to access SMM CLI using Telnet or SSH. Only console access is supported using the chassis front panel console ports as described in the FortiGate-7000 system guide.

For monitoring purpose, IPMI over IP is supported on SMM Ethernet ports. See your FortiGate-7000 system guide for details.

FortiOS features not supported by FortiGate-7000 v6.0.4

The following mainstream FortiOS 6.0.4 features are not supported by the FortiGate-7000 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
```

- Hard disk features including, WAN optimization, web caching, explicit proxy content caching, disk logging, and GUI-based packet sniffing.
- The FortiGate-7000 platform only supports quarantining files to FortiAnalyzer.
- Log messages should be sent only using the management aggregate interface
- The FortiGate-7000 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-7000

For a list of new FortiOS 6.0.4 FortiGate-7000 IPsec VPN features and a list of IPsec VPN features not supported by FortiOS 6.0.4 FortiGate-7000 IPsec VPN, see FortiGate-7000 IPsec VPN on page 66.

SSL VPN

Sending all SSL VPN sessions to the primary FPM 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 FPM.
- Creating flow rules that send all sessions that use the SSL VPN IP pool addresses to the primary FPM.

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 55.

Traffic shaping and DDoS policies

Each FPM applies traffic shaping and DDoS quotas independently. Because of load-balancing, this may allow more traffic than expected.

FortiGuard web filtering

All FortiGuard rating queries are sent through management aggregate interface from the management VDOM (named mgmt).

Log messages include a slot field

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

FortiOS Carrier

You have to apply a FortiOS Carrier license separately to each FIM and FPM to license a FortiGate-7000 for FortiOS Carrier.

Special notice for new deployment connectivity testing

Only the primary FPM can successfully ping external IP addresses. During a new deployment, while performing connectivity testing from the Fortigate-7000, make sure to run `execute ping` tests from the primary FPM CLI.

FortiGate-7000 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 | <FPM#>}
      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`.

set 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.

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 | <FPM#>}

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

Where:

`master` forwards traffic to the primary FPM.

`all` means forward the traffic to all FPMs.

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

`<FPM#>` forward the matching traffic to a specific FPM. For example, FPM3 is the FPM 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 mgmt
   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 mgmt

Selects the interface used for management connections. For the FortiGate-7000, this option is always set to `mgmt` and cannot be changed. The IP address of this interface (`mgmt`) becomes the IP address used to enable management access to individual FPMs using special administration ports as described in Managing individual FPMs on page 1. To manage individual FPCs, this interface must be connected to a network.

max-miss-heartbeats <heartbeats>

Set the number of missed heartbeats before an FPM is considered to have failed. If a failure occurs, the DP2 processor will no longer load balance sessions to the FPM.

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 FPM is considering to have failed. If a failure occurs, the DP2 processor will no longer load balance sessions to the FPM.

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-7000 directs IPsec VPN sessions to the DP2 processors which load balance them among the FPMs.

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-7000 will drop IPsec VPN sessions traveling between two IPsec tunnels because the two IPsec tunnels may be terminated on different FPMs. If you have traffic entering the FortiGate-7000 from one IPsec VPN tunnel and leaving the FortiGate-7000 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-U load balancing. If GTP-U load balancing is enabled, Tunnel Endpoint Identifiers (TEIDs) are used to identify GTP-U 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 FPMs. 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 FPM. This method is for troubleshooting only and should not be used for normal operation. Directing all sessions to the primary FPM will have a negative impact on performance.

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

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

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

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

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

`src-dst-ipsport-dport` distribute sessions across all FPMs 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 FPMs. 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) FPM.

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

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

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

`src-dst-ip` ICMP sessions are distributed across all FPMs 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 (FPM). Use the edit command to specify the slot the FPM is installed in. You can enable or disable each FPM and set a weight for each FPM.

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
```

FortiGate-7000 execute CLI commands

This chapter describes the FortiGate-7000 execute commands. Many of these commands are only available from the FIM CLI.

execute load-balance console-mgmt {disable | enable}

Enable or disable the console disconnect command on the management module CLI. If the console disconnect command is enabled, you can log into one of the management module consoles and use the console disconnect command to disconnect the other management module console.

The FortiGate-7000 management module has two consoles that you can use to connect to the management module CLI or to the CLIs of any of the FIMs or FPMs in the FortiGate-7000 system. However, the system only supports one console connection to a module at a time. So if the other management module console is connected to an FIM or FPM that you want to connect to, you have to disconnect the other management module console to be able to connect to the FIM or FPM.

To disconnect the other management module console, you can log into the management module CLI and use the console disconnect command to disconnect the other console.

You can use this command to enable or disable this functionality.

execute load-balance console-mgmt disconnect <console>

Disconnect one of the management module consoles from the FIM or FPM that it is connected to. `<console>` is the number of the console to disconnect.

This command allows you to disconnect a management module console session from the FIM CLI without having to log into the management module CLI.

execute load-balance console-mgmt info

This command shows whether the management module console disconnect command is enabled or disabled and also shows which modules the management module consoles are connected to or if they are disconnected.

execute load-balance license-mgmt list

List the licenses that have been added to this FortiGate-7000, including a license for extra VDOMs and FortiClient licenses.

execute load-balance license-mgmt reset {all | crypto-key | forticlient | vdom}

Reset licenses and crypto keys added to this FortiGate-7000. Enter `all` to reset all licenses and crypto keys. Resetting `all`, `crypto-key`, or `vdom` reboots the FortiGate-7000, which starts up with the specified licenses set to default values and, if applicable, re-generates crypto keys while restarting. Resetting `forticlient` requires you to manually restart the FortiGate-7000 before the change takes affect.

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

Log into the CLI of an individual FIM or FPM. Use `<slot>` to specify the FIM or FPM 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 power-off <slot-map>

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

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

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

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

execute load-balance slot reboot <slot-map>

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