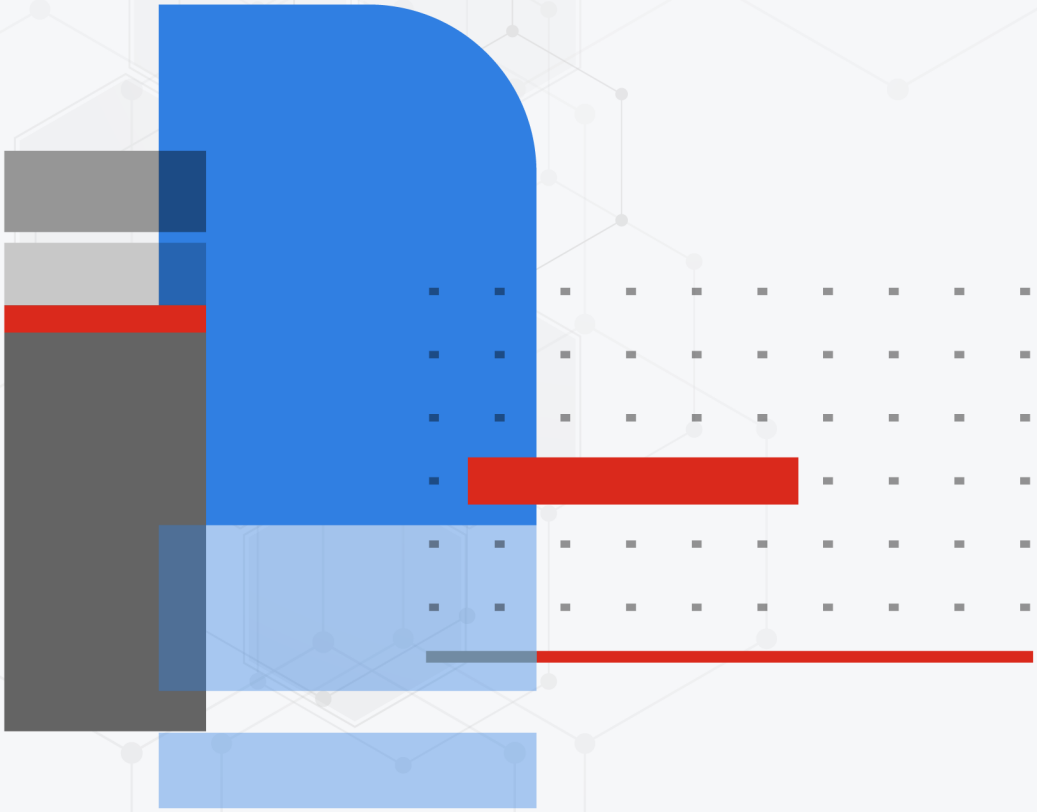
FortiGate-7000E Administration Guide

FortiOS 7.4.0



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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 25, 2023
FortiOS 7.4.0 FortiGate-7000E Administration Guide
01-740-396655-20230825

TABLE OF CONTENTS

Change log

Date	Change description
August 25, 2023	The section Enabling GTP load balancing on page 49 now describes the correct load balancing configuration for optimal GTP performance.
August 9, 2023	New section: FortiGate-7000E and FortiOS Carrier on page 35. Removed incorrect information about FortiOS Carrier licensing.
July 24, 2023	New section, FortiGate-7000E IPsec load balancing EMAC VLAN interface limitation on page 114.
May 11, 2023	FortiOS 7.4.0 document release.

What's New

This section describes what's been added to FortiOS 7.4 FortiGate-7000E releases.

What's new for FortiGate-7000E 7.4.0

FortiGate-7000E for FortiOS 7.4.0 includes the following new features:

- Main branch support for the following FortiGate-7000E models:
  - FortiGate-7030E
  - FortiGate-7040E
  - FortiGate-7060E

FortiGate-7000E overview

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

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

The same FortiOS firmware build runs on each FIM and FPM in the chassis. You can upgrade FortiGate-7000E firmware by logging into the primary FIM and performing a firmware upgrade as you would for any FortiGate. During the upgrade process, the firmware of all of the FIMs and FPMs 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-7000E product is made up of a FortiGate-7000E series chassis, one or two FIMs and two to four FPMs. The entire package is licensed and configured as a single product under the FortiGate-7000E chassis serial number. When you receive a new FortiGate-7000E product, you register it on https://support.fortinet.com using the chassis serial number. Use the chassis serial number when requesting support from Fortinet.

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

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

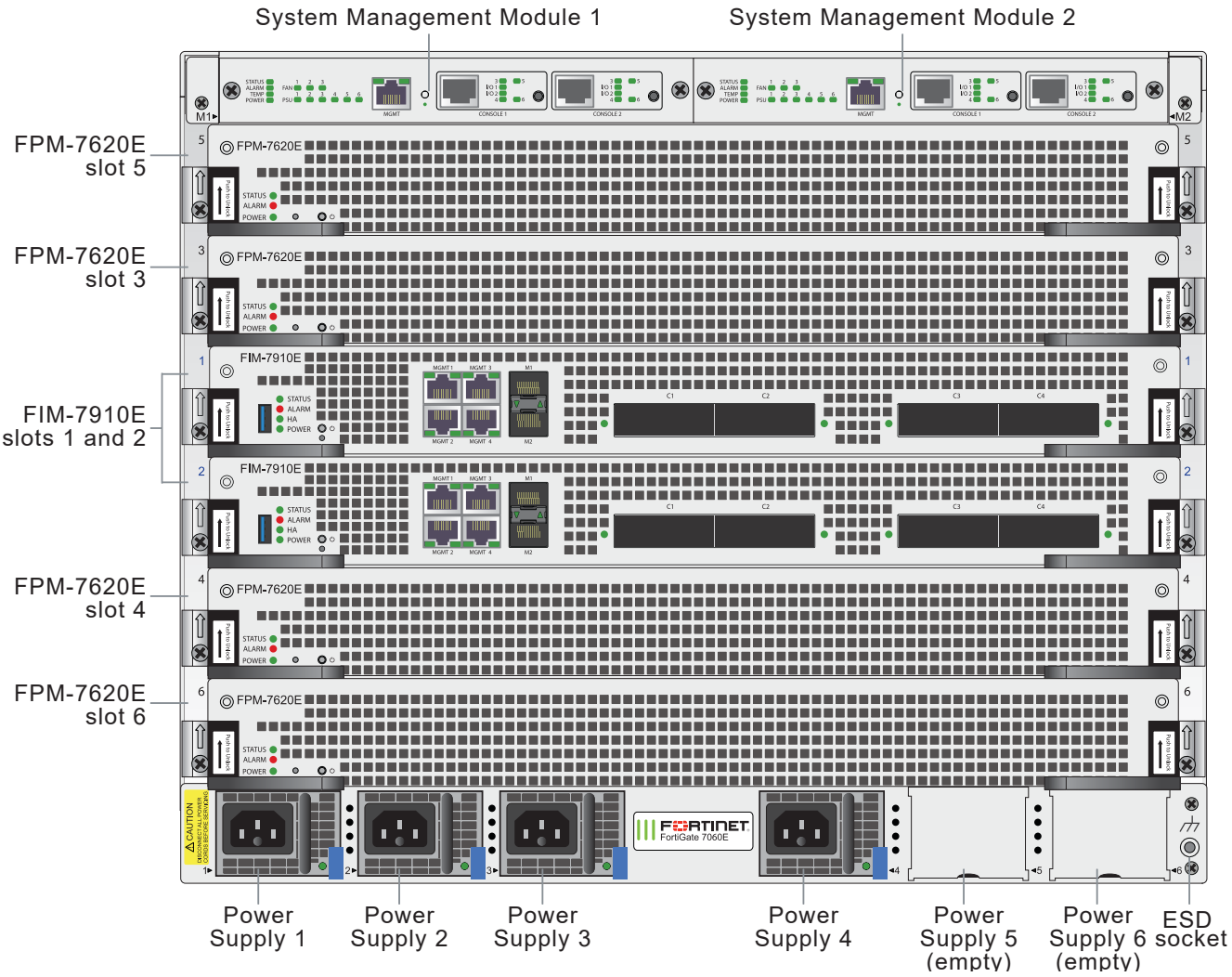
FortiGate-7060E

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 System Management Modules (SMM). 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 SMM 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)

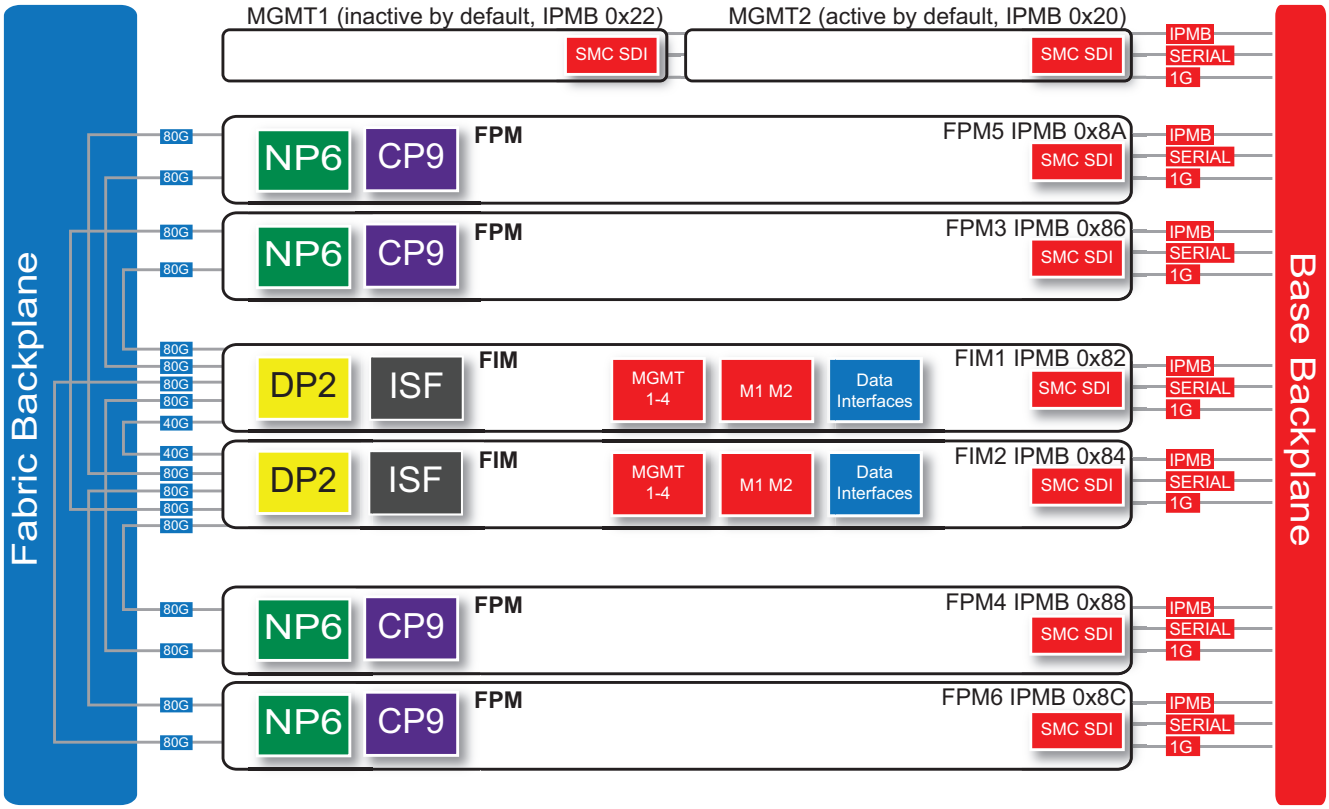


Power is provided to the chassis using four hot swappable 3+1 redundant 100-240 VAC, 50-60 Hz power supply units (PSUs). You can also optionally add up to six PSUs to provide 3+3 redundancy. The FortiGate-7060E can also be equipped with DC PSUs allowing you to connect the chassis to -48V DC power

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 SMMs (MGMT), the FIMs (called FIM1 and FIM2) and the FPMs (FPM3, FPM4, FPM5, and FPM6).



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

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

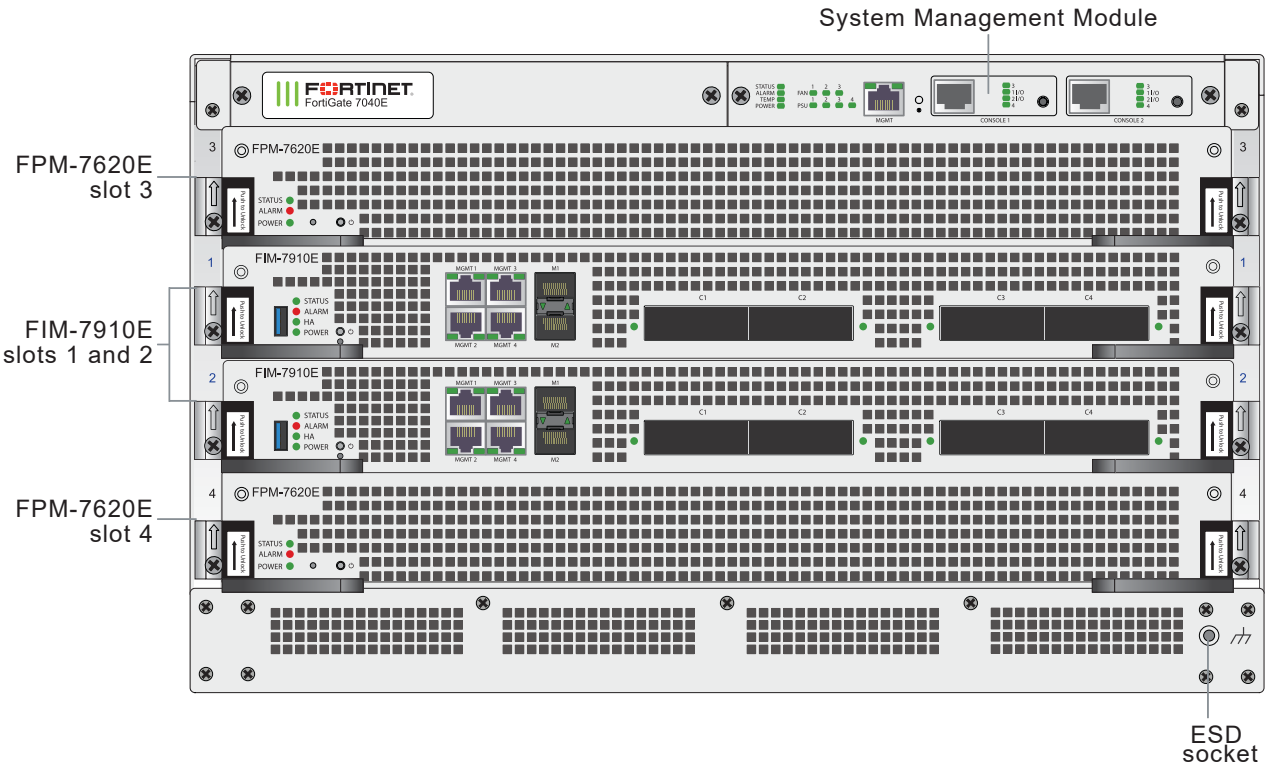
FortiGate-7040E

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

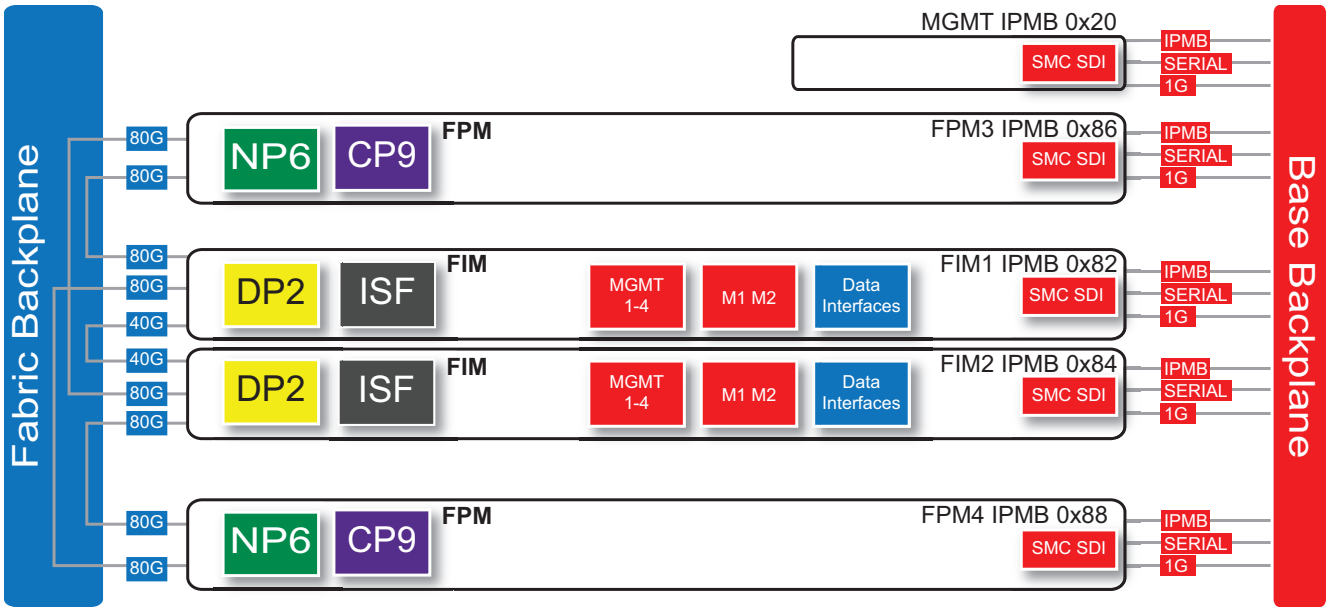
The FortiGate-7040E chassis is managed by a single System Management Module (SMM) that includes an Ethernet connection as well as two switchable console ports that provide console connections to the modules in the chassis slots. The SMM controls chassis cooling and power management and provides an interface 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 System Management Module (MGMT), the FIMs (called FIM1 and FIM2) and the FPMs (FPM3 and FPM4).



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

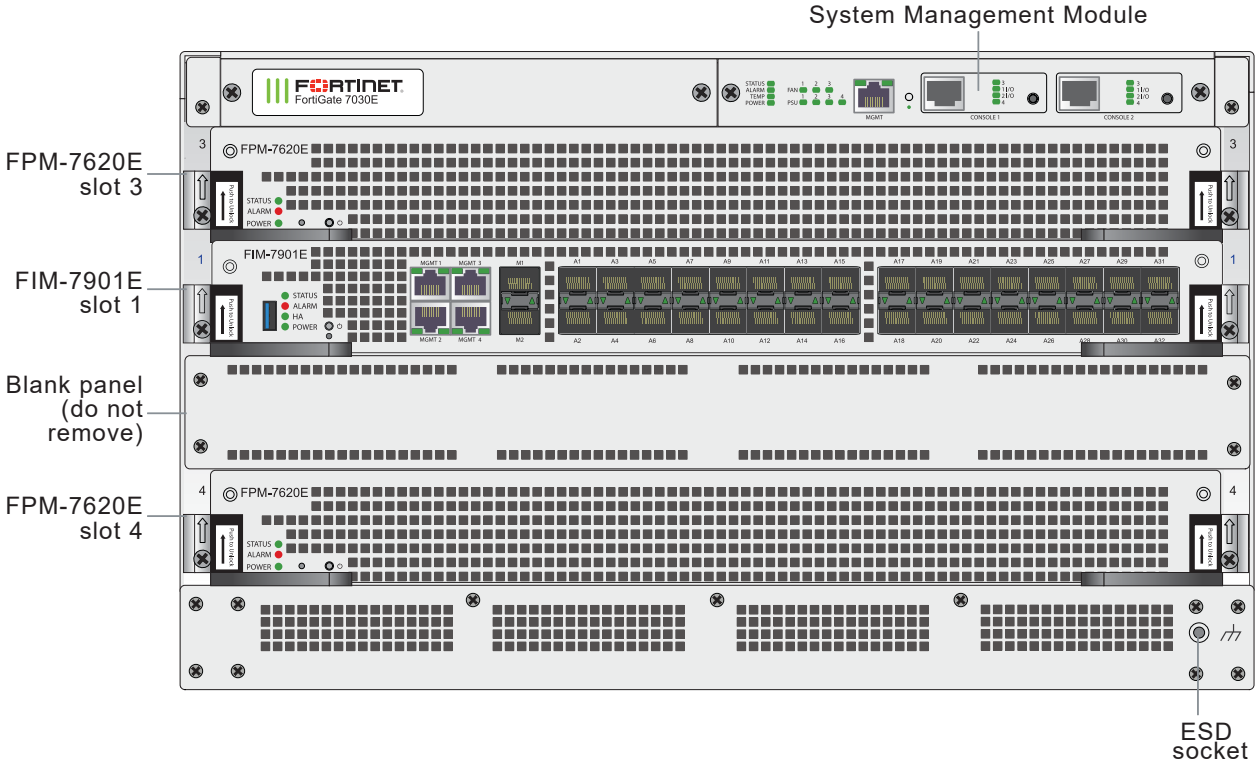
The FortiGate-7030E is a 6U 19-inch rackmount 3-slot chassis with a 80Gbps fabric and 1Gbps base backplane designed by Fortinet. The fabric backplane provides network data communication and the base backplane provides management and synch communication among the chassis slots.

FortiGate-7030E front panel

The FortiGate-7030E chassis is managed by a single System Management Module (SMM) that includes an Ethernet connection as well as two switchable console ports that provide console connections to the modules in the chassis slots. The SMM 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

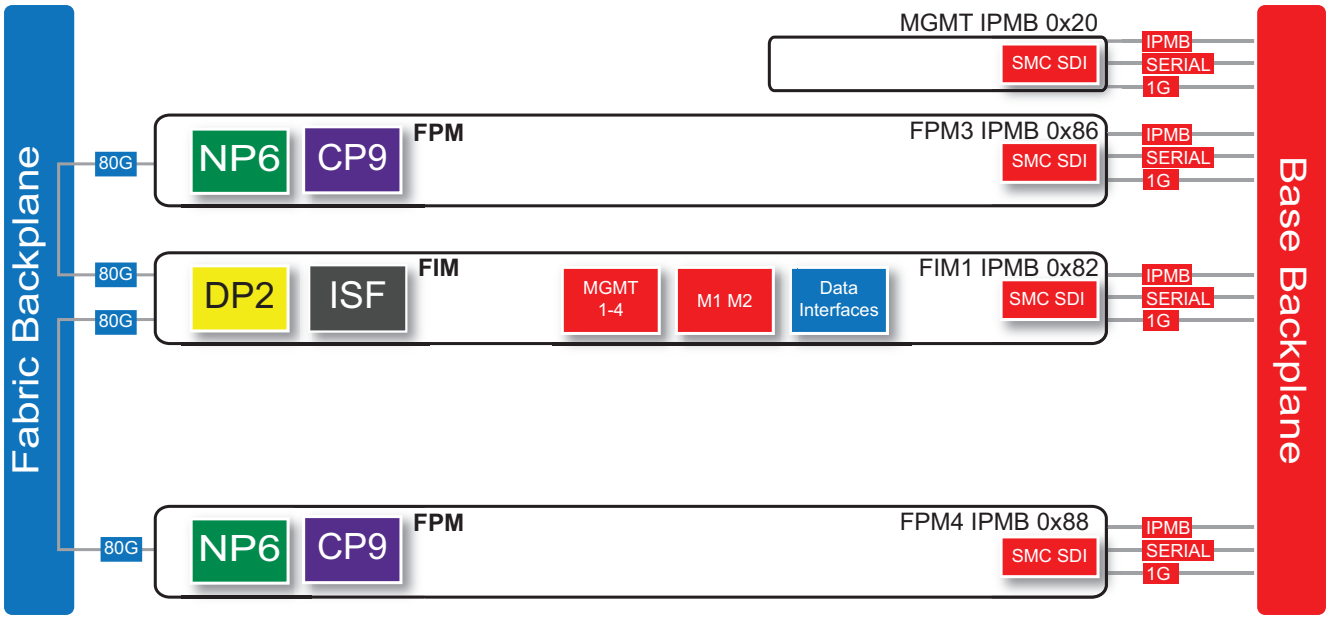
chassis slot 1 and two FPM (processing) modules in chassis slots 3 and 4. The front panel also includes a sealed blank panel. Breaking the seal or removing the panel voids your FortiGate-7030E warranty.

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 System Management Module (MGMT), the FIM (called FIM1) and the FPMs (FPM3 and FPM4).



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

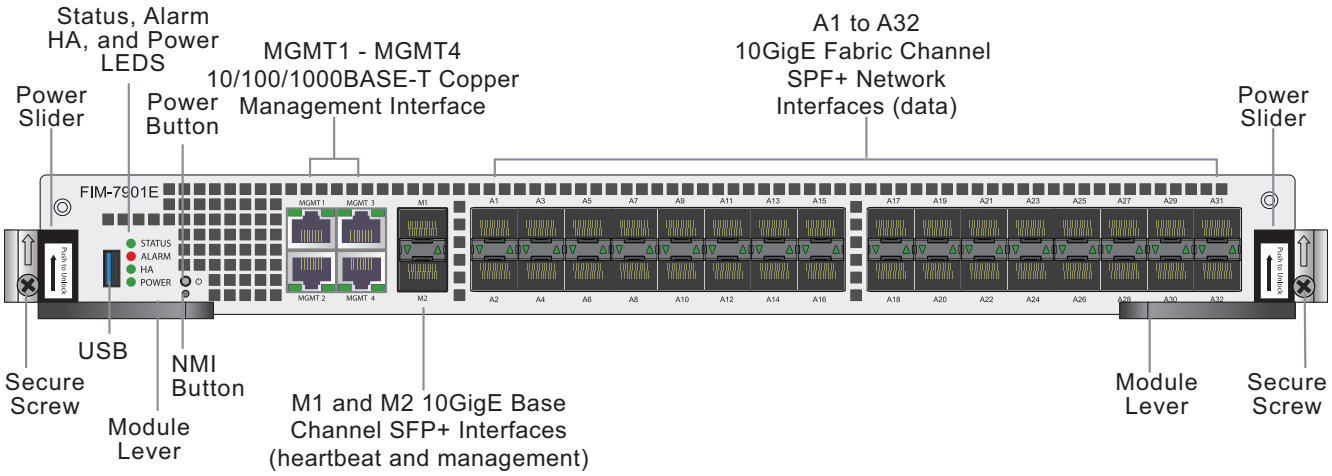
FIM-7901E interface module

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 7000E series 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 also includes a 1Gbps base backplane channel for base backplane management communication with each FPM module in the chassis, one 40Gbps fabric backplane channel for fabric backplane communication with the FIM module(s) in the chassis, and a second 1Gbps base backplane channel for base backplane communication with the FIM module(s) in the chassis.

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

You can also install FIM-7901Es in a second chassis and operate the chassis in HA mode to provide chassis failover protection.

FIM-7901E front panel



FIM-7901E front panel interfaces

You connect the FIM-7901E to your 10Gbps networks using the A1 to A32 front panel SFP+ interfaces. The front panel also includes M1 and M2 SFP+ interfaces for the base channel, four Ethernet management interfaces (MGMT1 to MGMT4), and a USB port. The USB port can be used with any USB key for backing up and restoring configuration files.

Connector	Type	Speed	Protocol	Description
A1 to A32	SPF+	10Gbps/1Gpbs	Ethernet	Thirty-two front panel 10GigE SFP+ fabric channel interfaces. 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.
M1 and M2	SFP+	10Gbps/1Gbps	Ethernet	Two front panel 10GigE SFP+ interfaces 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

Connector	Type	Speed	Protocol	Description
				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
MGMT1 to MGMT4	RJ-45	10/100/1000Mbps	Ethernet	Four 10/100/1000BASE-T copper out of band management Ethernet interfaces.
USB	USB 3.0 Type A		USB 3.0 USB 2.0	Standard USB connector.

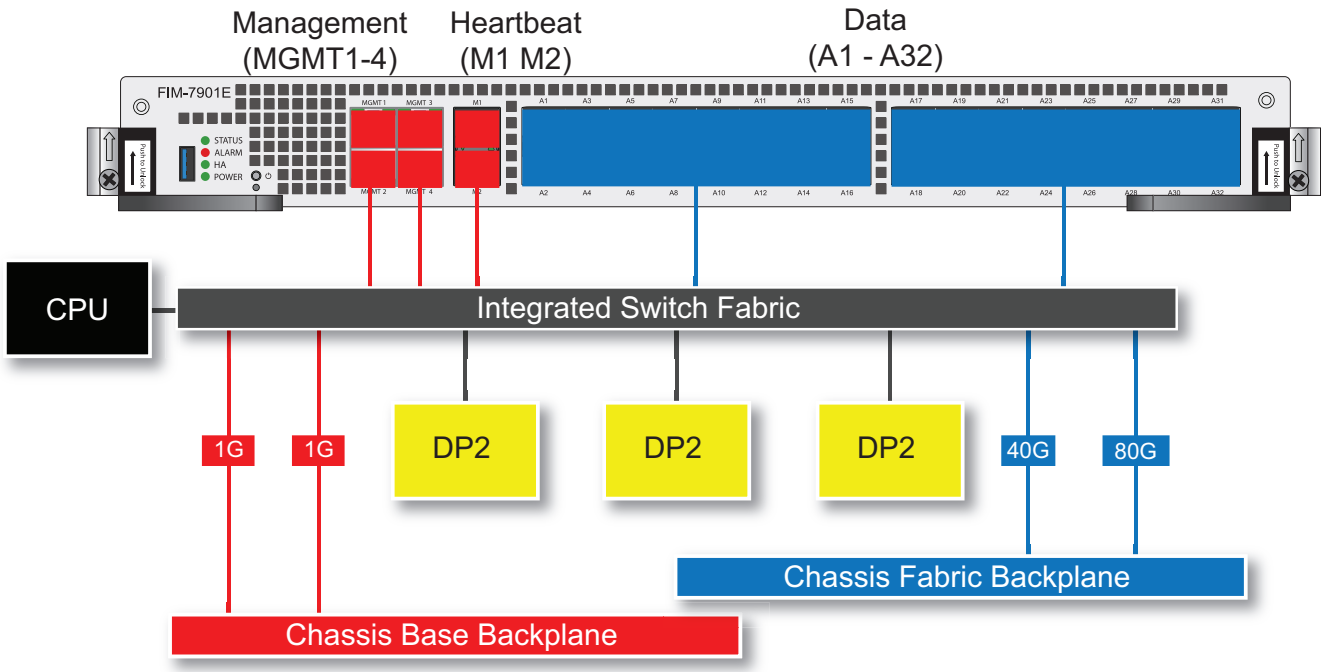
FIM-7901E schematic

The FIM-7901E 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 FPM modules in the same chassis.

The FIM-7901E also includes the following backplane communication channels:

- One 80Gbps fabric backplane channel to distribute traffic to the FPMs.
- One 1Gbps base backplane channel for base backplane communication with the FPMs.
- One 40Gbps fabric backplane channel for fabric backplane communication with the other FIM.
- One 1Gbps base backplane channel for base backplane communication with the other FIM.

FIM-7901E hardware architecture



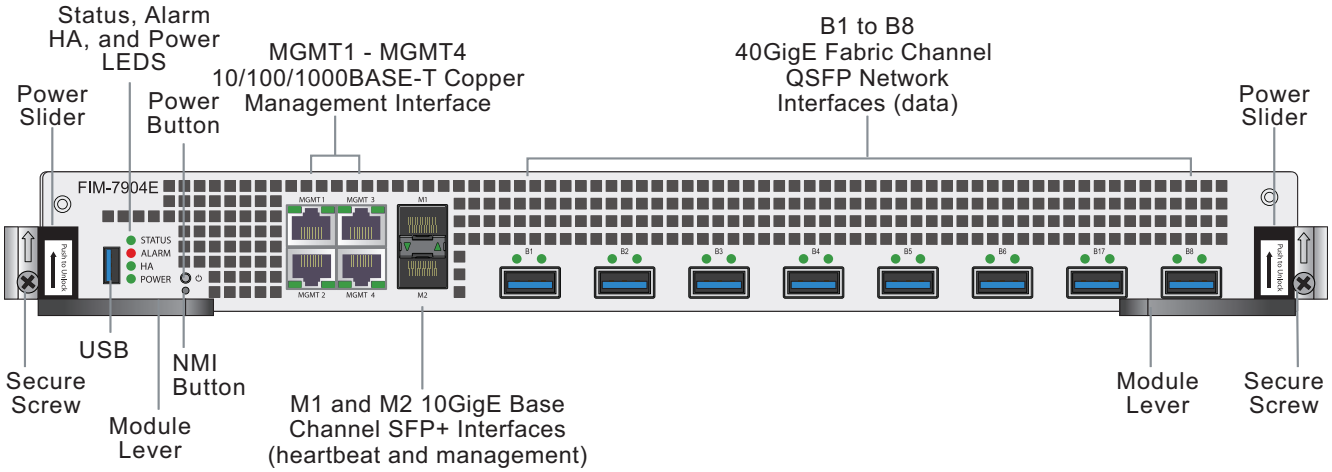
FIM-7904E interface module

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 7000E 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 also includes a 1Gbps base backplane channel for base backplane management communication with each FPM module in the chassis, one 40Gbps fabric backplane channel for fabric backplane communication with the FIM module(s) in the chassis, and a second 1Gbps base backplane channel for base backplane communication with the FIM module(s) in the chassis.

The FIM-7904E can be installed in any FortiGate 7000E series chassis in chassis hub/switch slots 1 or 2. The FIM-7904E provides four Quad Small Form-factor Pluggable plus (QSFP+) interfaces for a FortiGate 7000E 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 to provide chassis failover protection.

FIM-7904E front panel



FIM-7904E front panel interfaces

You connect the FIM-7904E to your 40Gbps networks using the B1 to B8 front panel QSFP+ interfaces. The front panel also includes M1 and M2 SFP+ interfaces for the base channel, four Ethernet management interfaces (MGMT1 to MGMT4), and a USB port. The USB port can be used with any USB key for backing up and restoring configuration files.

Connector	Type	Speed	Protocol	Description
B1 to B8	QSFP+	40Gbps/10Gbps	Ethernet	Eight front panel 40GigE QSFP+ fabric channel interfaces. These interfaces are connected to 40Gbps networks to distribute sessions to the FPM processor modules installed in chassis slots 3 and up. Using

Connector	Type	Speed	Protocol	Description
				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.
M1 and M2	SFP+	10Gbps/1Gbps	Ethernet	Two front panel 10GigE SFP+ interfaces 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
MGMT1 to MGMT4	RJ-45	10/100/1000Mbps	Ethernet	Four 10/100/1000BASE-T copper out of band management Ethernet interfaces.
USB	USB 3.0 Type A		USB 3.0 USB 2.0	Standard USB connector.

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 7000E system can be split into 4x10GBE interfaces. You split these interfaces after the FIM-7904Es are installed in your FortiGate 7000E system and the system is 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. Enabling, disabling, or changing the split interfaces configuration requires a system reboot. Fortinet recommends that you split multiple interfaces at the same time according to your requirements to avoid traffic disruption.

You should configure split interfaces or change interfaces types on both FortiGate-7000Es before forming an FGCP HA cluster. If you decide to change the split interfaces or interface type configuration after forming a cluster, you need to remove the backup FortiGate-7000E from the cluster and change interface configuration on both FortiGate-7000Es separately. After the FortiGate-7000Es restart, you can re-form the cluster. This process will cause traffic interruptions.

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 7000E 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 7000E 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.

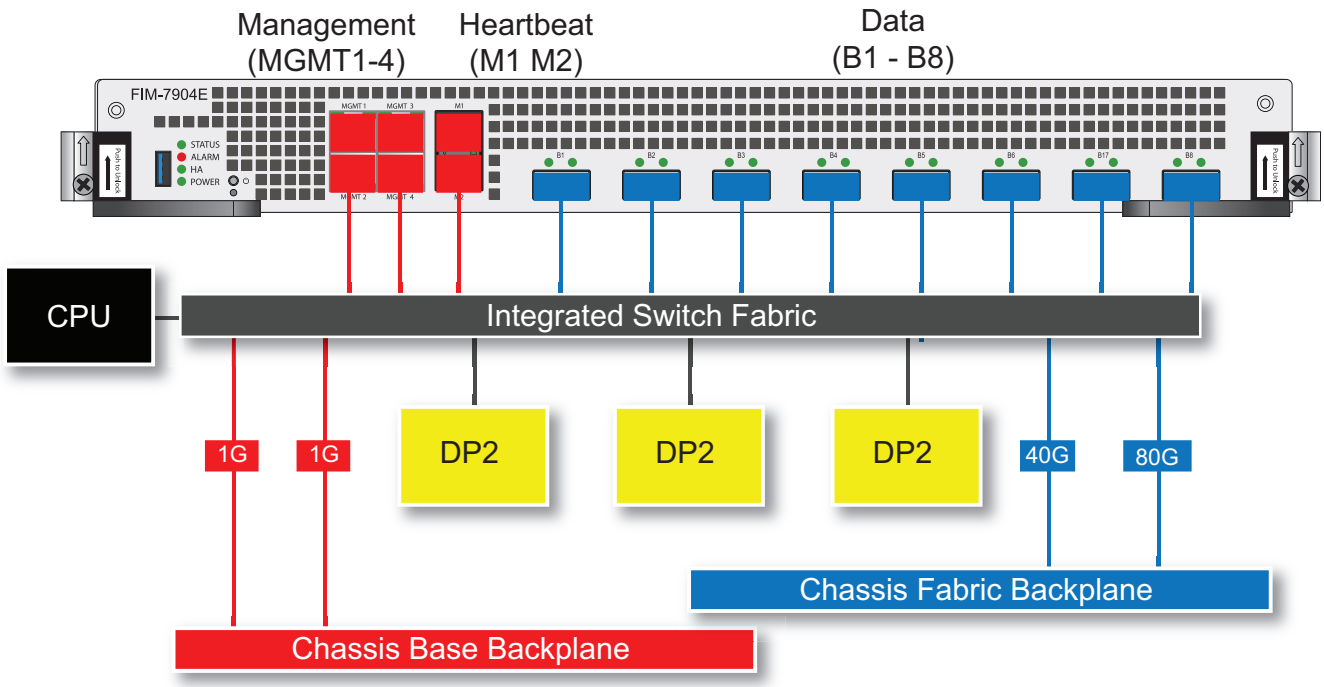
FIM-7904E hardware schematic

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 FPM modules in the same chassis.

The FIM-7904E also includes the following backplane communication channels:

- One 80Gbps fabric backplane channel to distribute traffic to the FPMs.
- One 1Gbps base backplane channel for base backplane communication with the FPMs.
- One 40Gbps fabric backplane channel for fabric backplane communication with the other FIM.
- One 1Gbps base backplane channel for base backplane communication with the other FIM.

FIM-7904E hardware architecture



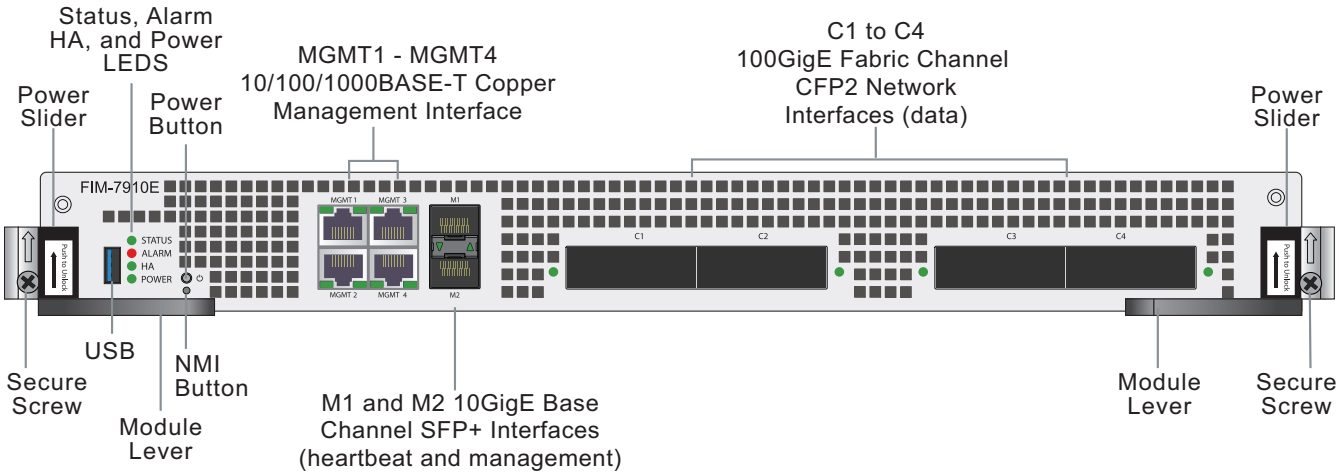
FIM-7910E interface module

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 7000E series chassis. The FIM-7910E includes an integrated switch fabric and DP2 processors to load balance millions of data sessions over the 80Gbps fabric backplane channel to FPM processor modules. The FIM-7910E also includes a 1Gbps base backplane channel for base backplane management communication with each FPM module in the chassis, one 40Gbps fabric backplane channel for fabric backplane communication with the FIM module(s) in the chassis, and a second 1Gbps base backplane channel for base backplane communication with the FIM module(s) in the chassis.

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

You can also install FIM-7910Es in a second chassis and operate the chassis in HA mode to provide chassis failover protection.

FIM-7910E front panel



FIM-7910E front panel interfaces

You connect the FIM-7910E to your 100Gbps networks using the C1 to C4 front panel CFP2 interfaces. The front panel also includes M1 and M2 SFP+ interfaces for the base channel, four Ethernet management interfaces (MGMT1 to MGMT4), and a USB port. The USB port can be used with any USB key for backing up and restoring configuration files.

Connector	Type	Speed	Protocol	Description
C1 to C4	CFP2	100Gbps/10Gbps	Ethernet	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 SFP+ interfaces. These interfaces also support creating link aggregation groups (LAGs) that can include interfaces from both FIM-7910Es.
M1 and M2	SFP+	10Gbps/1Gbps	Ethernet	Two front panel 10GigE SFP+ interfaces 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

Connector	Type	Speed	Protocol	Description
				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
MGMT1 to MGMT4	RJ-45	10/100/1000Mbps	Ethernet	Four 10/100/1000BASE-T copper out of band management Ethernet interfaces.
USB	USB 3.0 Type A		USB 3.0 USB 2.0	Standard USB connector.

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 7000E system can be split into 10 x 10GBE SFP+ interfaces. You split these interfaces after the FIM-7910Es are installed in your FortiGate 7000E 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. Enabling, disabling, or changing the split interfaces configuration requires a system reboot. Fortinet recommends that you split multiple interfaces at the same time according to your requirements to avoid traffic disruption.

You should configure split interfaces or change interfaces types on both FortiGate-7000Es before forming an FGCP HA cluster. If you decide to change the split interfaces or interface type configuration after forming a cluster, you need to remove the backup FortiGate-7000E from the cluster and change interface configuration on both FortiGate-7000Es separately. After the FortiGate-7000Es restart, you can re-form the cluster. This process will cause traffic interruptions.

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 7000E 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 7000E 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.

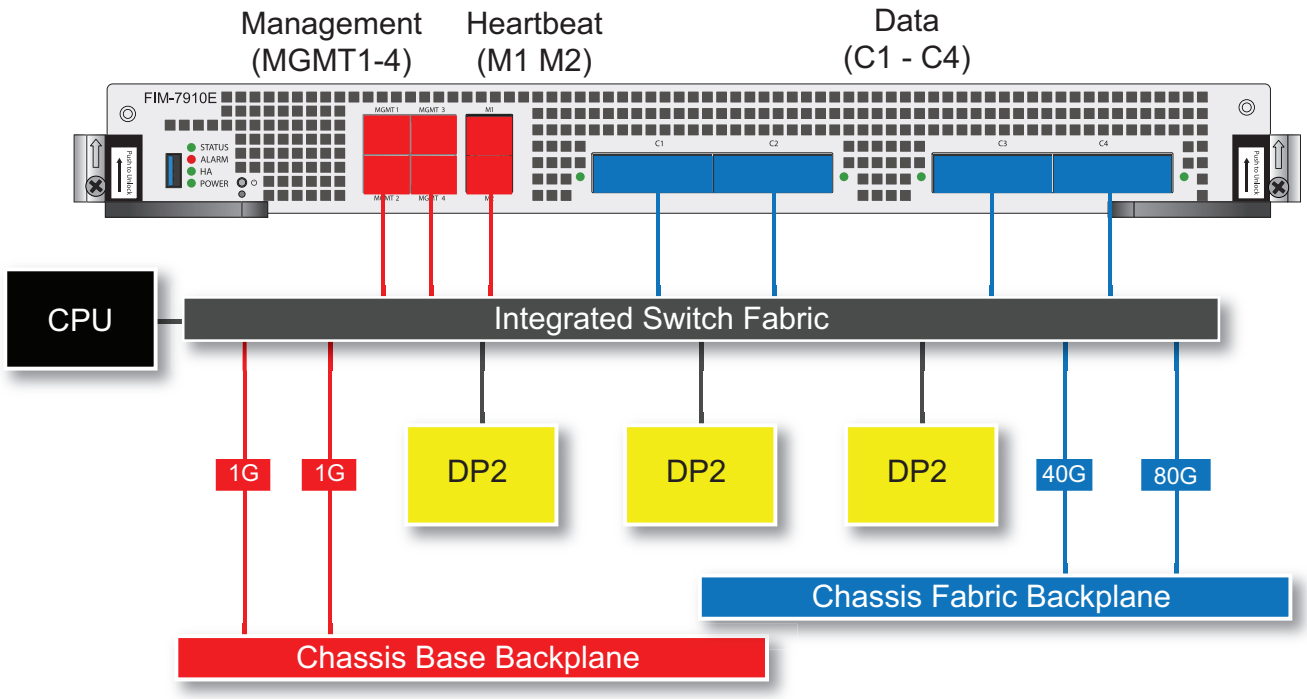
FIM-7910E hardware schematic

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 FPM modules in the same chassis.

The FIM-7910E also includes the following backplane communication channels:

- One 80Gbps fabric backplane channel to distribute traffic to the FPMs.
- One 1Gbps base backplane channel for base backplane communication with the FPMs.
- One 40Gbps fabric backplane channel for fabric backplane communication with the other FIM.
- One 1Gbps base backplane channel for base backplane communication with the other FIM.

FIM-7910E hardware architecture



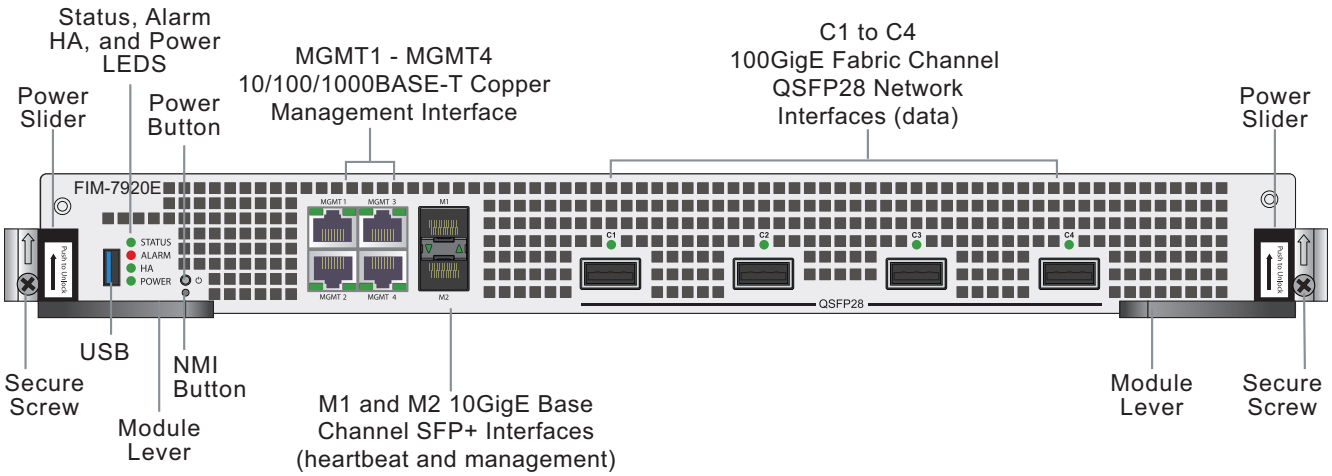
FIM-7920E interface module

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 7000E series chassis. The FIM-7920E includes an integrated switch fabric and DP2 processors to load balance millions of data sessions over the 80Gbps fabric backplane channel to FPM processor modules. The FIM-7920E also includes a 1Gbps base backplane channel for base backplane management communication with each FPM module in the chassis, one 40Gbps fabric backplane channel for fabric backplane communication with the FIM module(s) in the chassis, and a second 1Gbps base backplane channel for base backplane communication with the FIM module(s) in the chassis.

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

You can also install FIM-7920Es in a second chassis and operate the chassis in HA mode to provide chassis failover protection.

FIM-7920E front panel



FIM-7920E front panel interfaces

You connect the FIM-7920E to your 100Gbps networks using the C1 to C4 front panel QSFP28 interfaces. The front panel also includes M1 and M2 SFP+ interfaces for the base channel, four Ethernet management interfaces (MGMT1 to MGMT4), and a USB port. The USB port can be used with any USB key for backing up and restoring configuration files.

Connector	Type	Speed	Protocol	Description
C1 to C4	QSFP28	100Gbps/40Gbps/10Gbps	Ethernet	Four front panel 100GigE QSFP28 fabric channel interfaces that can be 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 multiple FIM-7920Es.

Connector	Type	Speed	Protocol	Description
M1 and M2	SFP+	10Gbps/1Gbps	Ethernet	Two front panel 10GigE SFP+ interfaces 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
MGMT1 to MGMT4	RJ-45	10/100/1000Mbps	Ethernet	Four 10/100/1000BASE-T copper out of band management Ethernet interfaces.
USB	USB 3.0 Type A		USB 3.0 USB 2.0	Standard USB connector.

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.

You should change the interface type and configure split interfaces on both FortiGate 7000Es before forming an FGCP HA cluster. If you decide to change the split interfaces configuration after forming a cluster, you need to remove the backup FortiGate 7000E from the cluster and change the split interfaces configuration on both FortiGate 7000Es separately. After the FortiGate 7000Es restart, you can re-form the cluster. This process will cause traffic interruptions.

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 7000E system using the management IP and enter the following command:

```
config system global
```

```
   set qsfp28-40g-port 1-C1
end
```

The FortiGate 7000E 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 7000E 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 7000E system can be split into 4 x 10GBE interfaces. You split these interfaces after the FIM-7920Es are installed in your FortiGate 7000E system and the system is 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. Enabling, disabling, or changing the split interfaces configuration requires a system reboot. 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 7000E 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 7000E 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

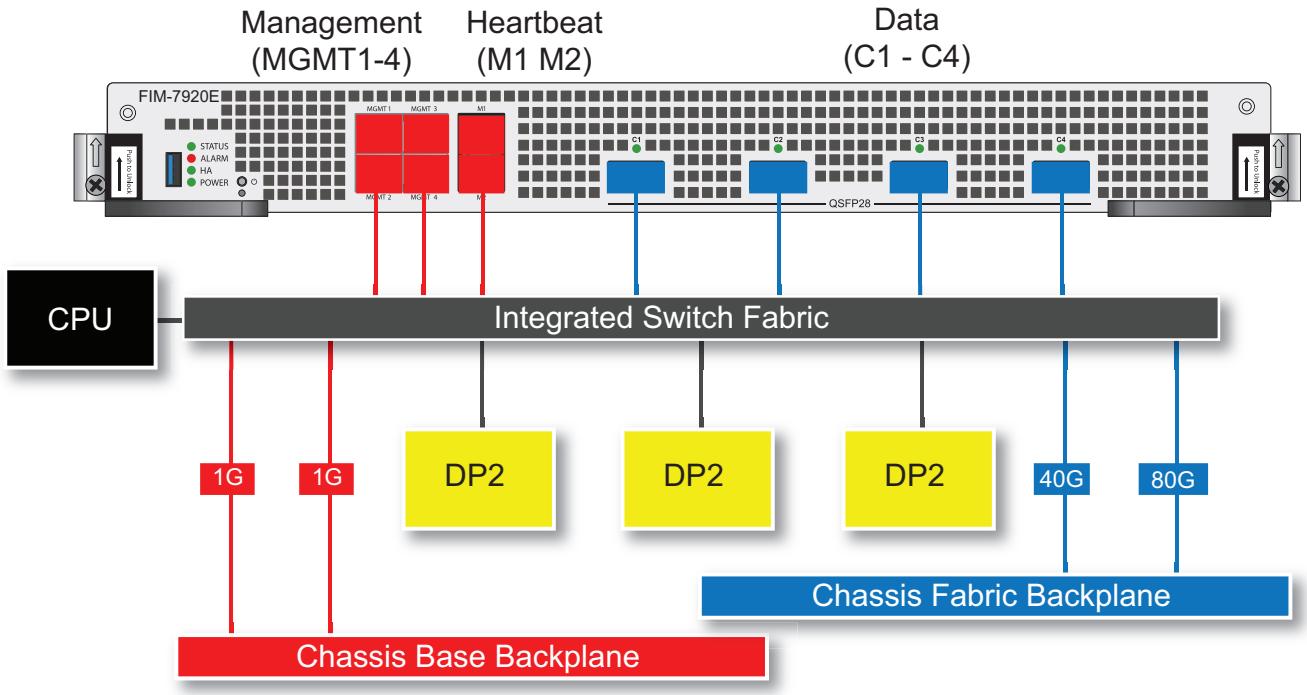
The FIM-7920E includes an integrated switch fabric (ISF) that connects the front panel interfaces to the DP2 session-aware load balancers and to the chassis backplanes. The ISF also allows the DP2 processors to distribute sessions among all NP6 processors on the FPM modules in the same chassis.

The FIM-7920E also includes the following backplane communication channels:

- One 80Gbps fabric backplane channel to distribute traffic to the FPMs.
- One 1Gbps base backplane channel for base backplane communication with the FPMs.

- One 40Gbps fabric backplane channel for fabric backplane communication with the other FIM.
- One 1Gbps base backplane channel for base backplane communication with the other FIM.

FIM-7920E hardware architecture



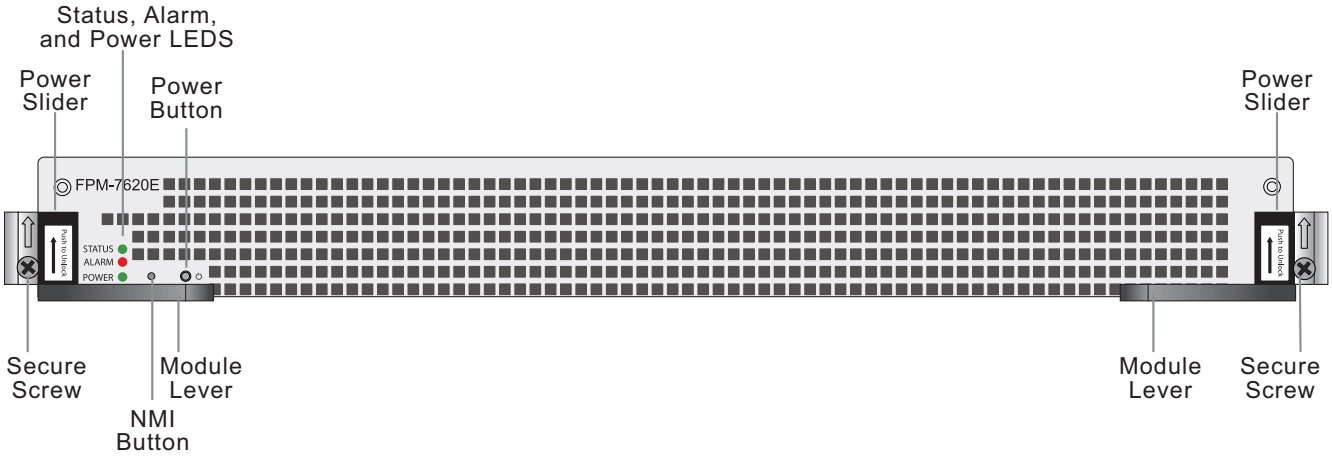
FPM-7620E processing module

The FPM-7620E processing module is a high-performance worker module that processes sessions load balanced to it by FortiGate 7000E series interface (FIM) modules over the chassis fabric backplane. The FPM-7620E can be installed in any FortiGate 7000E 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 four NP6 processors, and accelerates content processing with eight 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.

You can mix FPM-7620Es and FPM-7630Es in the same FortiGate 7000E chassis. In an HA configuration, both chassis in the HA cluster must have the same FPM modules in the same slots.

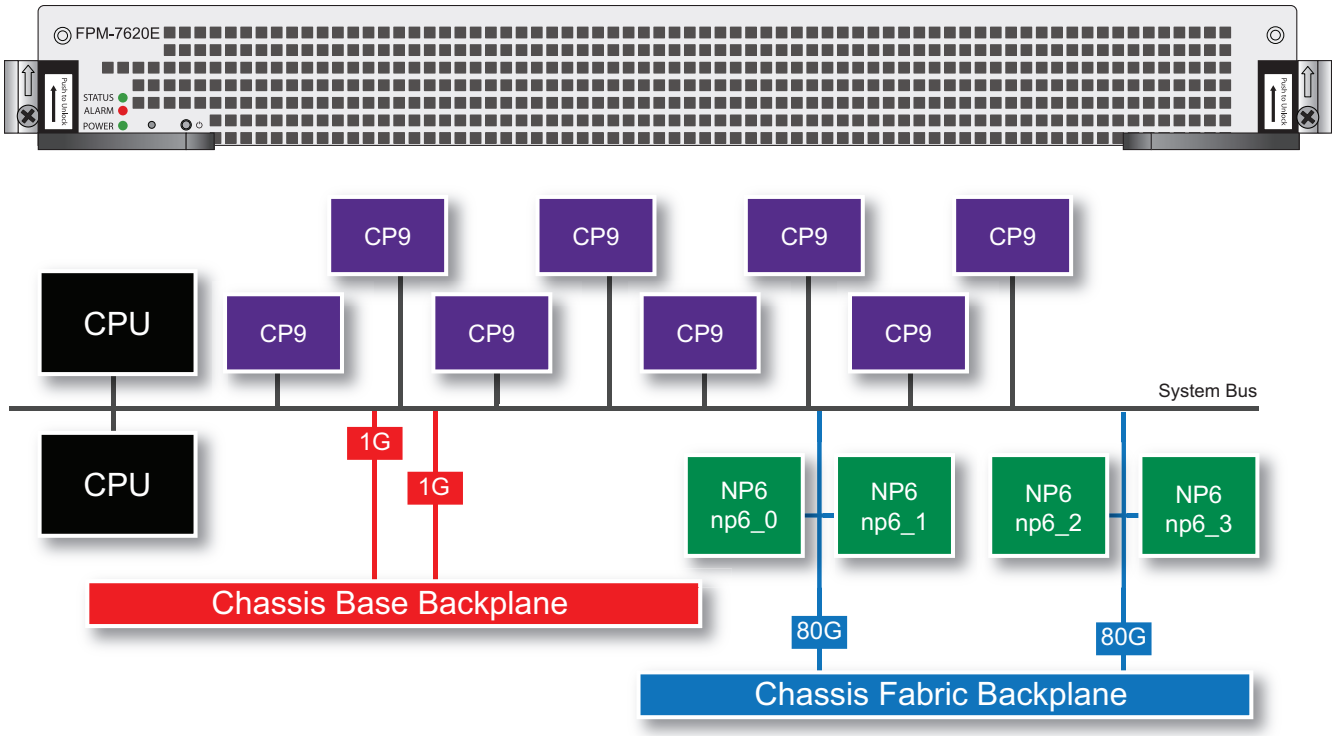
FPM-7620E front panel



FPM-7620E hardware schematic

The four FPM-7620E NP6 network processors, eight CP9 processors, and FIM module integrated switch fabric (ISF) provide hardware acceleration by offloading data traffic from the FPM-7620E CPUs. The result is enhanced network performance provided by the NP6 processors plus the network processing load is removed from the CPU. The NP6 processor can also handle some CPU intensive tasks, like IPsec VPN encryption/decryption. Because of the integrated switch fabric, all sessions are fast-pathed and accelerated.

FPM-7620E hardware architecture



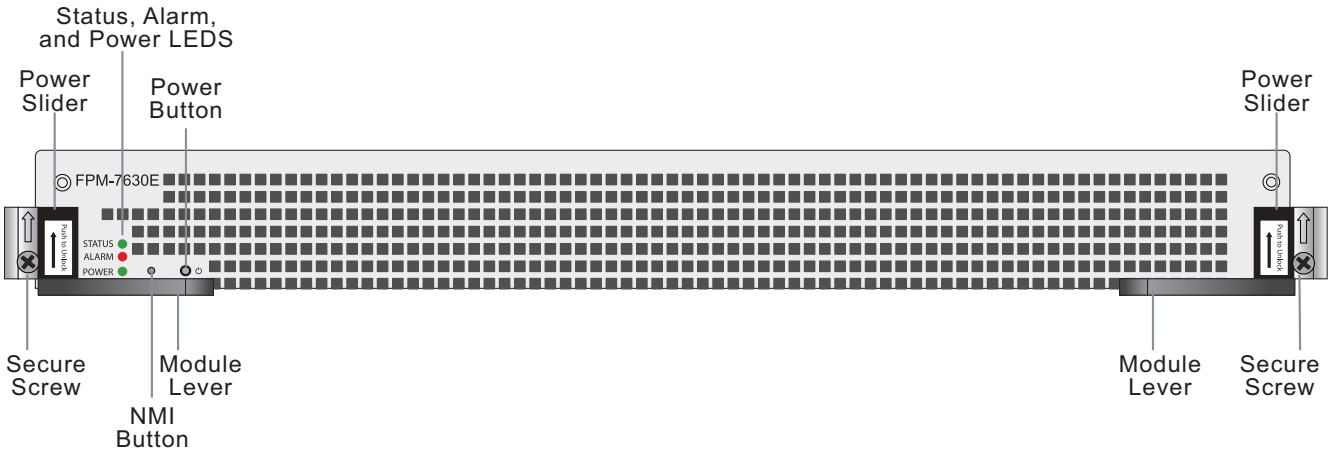
FPM-7630E processing module

The FPM-7630E processing module is a high-performance worker module that processes sessions load balanced to it by FortiGate 7000E series interface (FIM) modules over the chassis fabric backplane. The FPM-7630E can be installed in any FortiGate 7000E series chassis in slots 3 and up.

The FPM-7630E includes two 80Gbps connections to the chassis fabric backplane and two 1Gbps connections to the base backplane. The FPM-7630E processes sessions using a dual CPU configuration, accelerates network traffic processing with four NP6 processors, and accelerates content processing with eight 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-7630E processor module is an update of the FPM-7620E processor module with the same architecture but a newer CPU configuration. You can mix FPM-7630Es and FPM-7620Es in the same FortiGate 7000E chassis. In an HA configuration, both chassis in the HA cluster must have the same FPM modules in the same slots.

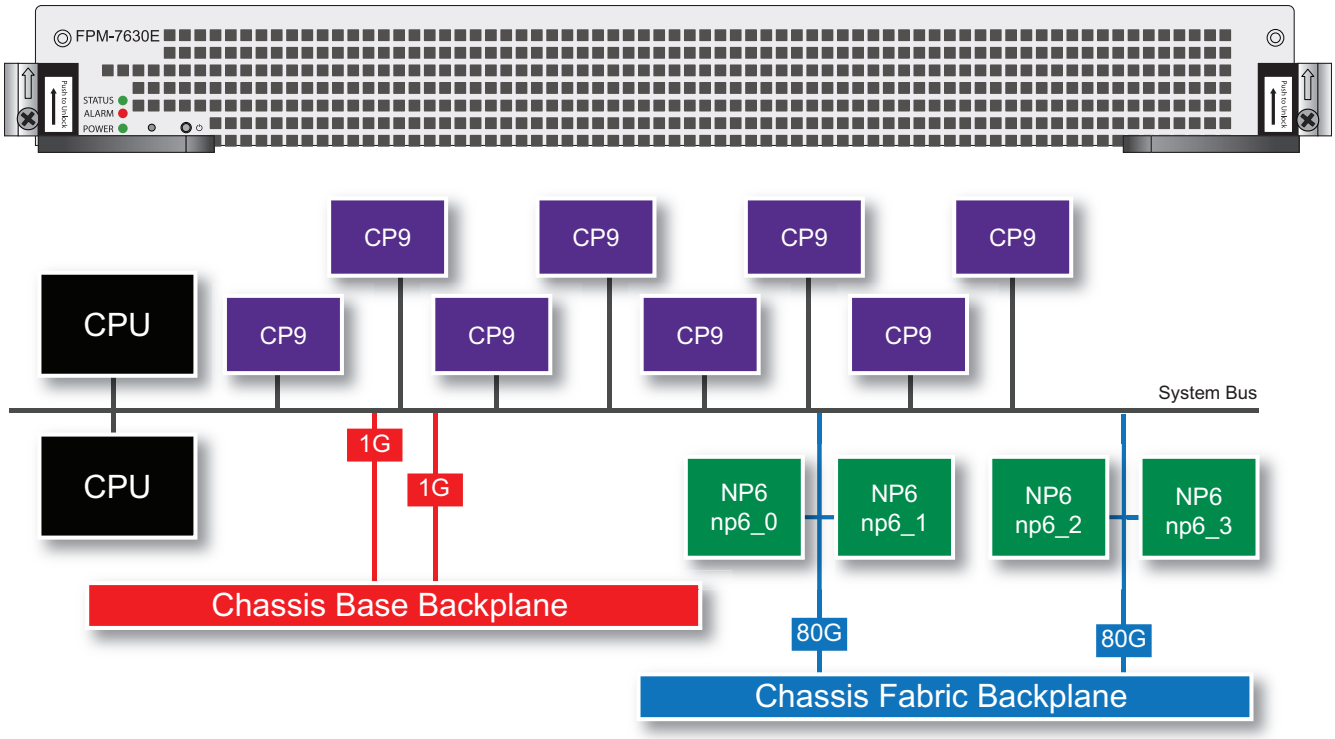
FPM-7630E front panel



FPM-7630E hardware schematic

The four FPM-7630E NP6 network processors, eight CP9 processors, and FIM module integrated switch fabric (ISF) provide hardware acceleration by offloading data traffic from the FPM-7630E CPUs. The result is enhanced network performance provided by the NP6 processors plus the network processing load is removed from the CPU. The NP6 processor can also handle some CPU intensive tasks, like IPsec VPN encryption/decryption. Because of the integrated switch fabric, all sessions are fast-pathed and accelerated.

FPM-7630E hardware architecture



Getting started with FortiGate-7000E

Begin by installing your FortiGate-7000E chassis in a rack and installing FIMs and FPMs 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 FortiGate-7000E will not allow traffic to pass through and you may not be able to log into the GUI or CLI. If you manage to log in, the session could time out as the FortiGate-7000E continues starting up.

Review the PSU, fan tray, System Management Module (SMM), 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.

When the chassis has initialized, you have a few options for connecting to the FortiGate-7000E 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.
- Log in to the primary FIM CLI by connecting to the RJ-45 RS-232 Console 1 serial port on the System Management Module (SMM) with settings: BPS: 9600, data bits: 8, parity: none, stop bits: 1, flow control: none.

The FortiGate-7000E 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-7000E to your network.
	From the GUI, access the Global GUI and go to **System > Administrators**, edit the **admin** account, and select **Change Password**.
	From the CLI:
	`config global`
	`  config system admin`
	`  edit admin`
	`  set password <new-password>`
	`  end`

FIM in slot 1	MGMT1: FIM01, 1-mgmt1, default IP address 192.168.1.99/24 (the MGMT1 interface is part of the mgmt redundant interface that also includes MGMT2, MGMT3, and MGMT4).
FIM in slot 2	MGMT2: FIM02, 2-mgmt1, default IP address 192.168.2.99/24 (the MGMT1 interface is part of the mgmt redundant interface that also includes MGMT2, MGMT3, and MGMT4).
If you choose to only install one FIM, it should be installed in slot 1.	MGMT1: FIM01, 1-mgmt1, default IP address 192.168.1.99/24

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

Confirming startup status

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

The FortiGate-7000E uses the Fortinet Security Fabric for communication and synchronization between the FIMs and the FPMs and for normal GUI operation. By default, the Security Fabric is enabled and must remain enabled for 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, Secondary, uptime=53740.68, priority=2, slot_id=2:2, idx=3, flag=0x10, in_sync=1
FIM04E3E16000010, Secondary, uptime=53790.94, priority=3, slot_id=1:1, idx=0, flag=0x10, in_sync=1
FIM04E3E16000014, Primary, uptime=53781.29, priority=1, slot_id=2:1, idx=1, flag=0x10, in_sync=1
FIM10E3E16000040, Secondary, uptime=53707.36, priority=4, slot_id=1:2, idx=2, flag=0x10, in_sync=1
FPM20E3E16900234, Secondary, uptime=53790.98, priority=16, slot_id=2:3, idx=4, flag=0x64, in_sync=1
FPM20E3E16900269, Secondary, uptime=53783.67, priority=17, slot_id=2:4, idx=5, flag=0x64, in_sync=1
FPM20E3E17900113, Secondary, uptime=53783.78, priority=116, slot_id=1:3, idx=6, flag=0x64, in_sync=1
FPM20E3E17900217, Secondary, uptime=53784.11, priority=117, slot_id=1:4, idx=7, flag=0x64, in_sync=1
...
```

FortiGate-7000E and the Security Fabric

The FortiGate-7000E supports the Fortinet Security Fabric and all Security Fabric related features. You can set up the FortiGate-7000E to serve as the Security Fabric root and you can configure the FortiGate-7000E to join an existing Security Fabric. For more information see Fortinet Security Fabric.

The FortiGate-7000E uses the Fortinet Security Fabric for communication and synchronization between the primary FIM and the FPMs and for normal GUI operation. By default, the Security Fabric is enabled and must remain enabled for normal operation.

When adding a FortiGate-7000E to an existing security fabric, for normal operation you must authorize the FortiGate-7000E and all of the FIMs and FPMs on the root FortiGate. Otherwise, the primary FIM will not be able to communicate with the other FIM and the FPMs.

You must also manually add a FortiAnalyzer to the FortiGate-7000E configuration, because the default FortiGate-7000E Security Fabric configuration has `configuration-sync` set to `local`, so the FortiGate-7000E doesn't get security fabric configuration settings, such as the FortiAnalyzer configuration, from the root FortiGate.

If the FortiGate-7000E is not joining a Security Fabric, Fortinet recommends that you do not change the Security Fabric configuration. You can verify the default Security Fabric configuration from the CLI:

```
config system csf
   set status enable
   set upstream 0.0.0.0
   set upstream-port 8013
   set group-name "SLBC"
   set group-password <password>
   set accept-auth-by-cert enable
   set log-unification disable
   set authorization-request-type serial
   set fabric-workers 2
   set downstream-access disable
   set configuration-sync local
   set fabric-object-unification default
   set forticloud-account-enforcement enable
end
```

FortiGate-7000E and FortiOS Carrier

To run FortiOS Carrier for FortiGate-7000E you must purchase a FortiOS Carrier license from Fortinet. A single FortiOS Carrier license is required for a FortiGate-7000E chassis. You apply the FortiOS Carrier license from the primary FIM CLI and the license is copied to the secondary FIM and to the FPMs.

Once you have a license key, you should upgrade your FortiGate-7000E chassis to the FortiOS software version that you want to be running and then use the following command from the primary FIM CLI to license your chassis for FortiOS Carrier:

```
execute forticarrier-license <license-key>
```

The FortiGate-7000E restarts and is set to the FortiOS Carrier factory default configuration. You can configure and operate a FortiGate-7000E running FortiOS Carrier just like a normal FortiGate-7000E. For example, you can upgrade the firmware by downloading and installing a new FortiOS firmware version or through FortiGuard. You do not have to re-license your FortiGate for FortiOS Carrier after installing new FortiOS firmware.

For more information about FortiOS Carrier, see the FortiOS Carrier Administration Guide.

For more information in this guide about FortiOS Carrier, see:

- GTP load balancing on page 49.
- PFCP load balancing on page 51.
- FortiGate-7000E FortiOS Carrier GTP with FGSP support on page 99.

Configuration synchronization

When you log into the FortiGate-7000E 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-7000E config-sync primary. 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 primary.

For the FortiGate-7000E to operate normally, the configurations of the FIMs and FPMs must be synchronized. You can use the information in the following sections to make sure that these configurations are synchronized

Confirming that the FortiGate-7000E is synchronized

You can use the following command to confirm that the configurations of the FIMs and FPMs are synchronized:

```
diagnose sys confsync status
```

The command shows the HA and configuration synchronization (confsync) status of the FIMs and FPMs. For each FIM and FPM, `in_sync=1` means the component is synchronized and can operate normally. If any component is out of sync, the command output will include `in_sync=0`. All components must be synchronized for the FortiGate-7000E to operate normally.

To confirm the configuration synchronization status of an HA cluster, see Confirming that the FortiGate-7000E HA cluster is synchronized on page 78.

FIM confsync status

The `diagnose sys confsync status` command output usually begins with the confsync status of the FIM in slot 2 and ends with the confsync status of the primary FIM (usually the FIM in slot 1). For each of the FIMs, the command output shows the configuration synchronization status with the other FIM and with each of the FPMs. The following example shows the configuration synchronization status of the FIM in slot 1, which is operating as the primary FIM:

```
Current slot: 1  Module SN: FIM01E3E17000165
ELBC: svcgrp_id=1, chassis=1, slot_id=1

ha zone: ha_primary_sn:FIM01E3E17000165, ha_primary_idx:1
Ha Member: FG74E43E17000073, mode=a-p, role=Primary, slot_id=1:1, idx=1, in_sync=1
Ha Member: FG74E43E17000065, mode=a-p, role=Secondary, slot_id=2:1, idx=0, in_sync=0

zone: self_idx:1, primary_idx:1, ha_primary_idx:1, members:4 ha_member:1
FIM01E3E17000165, Primary, uptime=70947.53, priority=1, slot_id=1:1, idx=1, flag=0x10, in_
sync=1
FIM04E3E16000102, Secondary, uptime=70948.25, priority=2, slot_id=1:2, idx=2, flag=0x10, in_
sync=0
       elbc-b-chassis: state=3(connected), ip=169.254.2.16, last_hb_time=71057.67, hb_nr=338183
FPM20E3E17900506, Secondary, uptime=70940.78, priority=20, slot_id=1:4, idx=3, flag=0x64,
in_sync=0
       elbc-b-chassis: state=3(connected), ip=169.254.2.4, last_hb_time=71057.78, hb_nr=338387
FPM20E3E17900511, Secondary, uptime=70940.69, priority=19, slot_id=1:3, idx=4, flag=0x64,
in_sync=0
       elbc-b-chassis: state=3(connected), ip=169.254.2.3, last_hb_time=71057.62, hb_nr=338456
```

FPM confsync status

The `diagnose sys confsync status` command output also lists the confsync status of each FPM. In the following example for a FortiGate-7040E, the output begins with the confsync status if the FPM in slot 3. The two lines that begin with serial numbers and end with `in_sync=1` indicate that the FPM (serial number FPM20E3E17900511) is synchronized with the primary FIM (serial number FIM01E3E17000165) and the primary FIM is synchronized with the FPM.

```
diagnose sys confsync status
...
Slot: 3  Module SN: FPM20E3E17900511
ELBC: svcgrp_id=1, chassis=1, slot_id=3
ELBC HB devs:
       elbc-ctrl/1: active=1, hb_count=70932
       elbc-ctrl/2: active=1, hb_count=70936
ELBC mgmt devs:
       elbc-b-chassis: mgmtip_set=1

zone: self_idx:2, primary_idx:0, ha_primary_idx:255, members:3
FPM20E3E17900511, Secondary, uptime=70940.69, priority=19, slot_id=1:3, idx=2, flag=0x4, in_
sync=0
FIM01E3E17000165, Primary, uptime=70947.53, priority=1, slot_id=1:1, idx=0, flag=0x10, in_
sync=1
       elbc-b-chassis: state=3(connected), ip=169.254.2.15, last_hb_time=71158.62, hb_nr=338046
FIM04E3E16000102, Secondary, uptime=70948.25, priority=2, slot_id=1:2, idx=1, flag=0x10, in_
sync=0
       elbc-b-chassis: state=3(connected), ip=169.254.2.16, last_hb_time=71158.62, hb_nr=338131
```

Viewing more details about FortiGate-7000E synchronization

If the output of the `diagnose sys configsync status` command includes `in_sync=0` entries, you can use the `diagnose sys confsync showcsum` command to view more details about the configuration checksums and potentially identify parts of the configuration that are not synchronized.

The `diagnose sys configsync showcsum` command shows HA and confsync debugzone and checksum information for the FIMs and FPMs, beginning with the FPM in slot 3 and ending with the primary FIM.

The following example shows the FPM in slot 3.

```
============================================================================
Slot: 3  Module SN: FPM20E3E17900511
ha debugzone
global: 7e 06 79 02 65 a9 ea e3 68 58 73 c2 33 d0 16 f1
root: 43 2c ee 2c f1 b3 b2 13 ff 37 34 5e 86 11 dc bf
mgmt-vdom: 9c 7d 58 9f 81 4b b7 4e ed 2a c3 02 34 b4 7c 63
all: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2

ha checksum
global: 7e 06 79 02 65 a9 ea e3 68 58 73 c2 33 d0 16 f1
root: 43 2c ee 2c f1 b3 b2 13 ff 37 34 5e 86 11 dc bf
mgmt-vdom: 9c 7d 58 9f 81 4b b7 4e ed 2a c3 02 34 b4 7c 63
all: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2

confsync debugzone
global: 09 28 1a fd 1b 4c 7d 39 1b 67 8a 62 e0 04 f8 b3
```

```
root: 8c 54 95 74 40 68 2c a7 3e ef e6 26 d3 37 09 08
mgmt-vdom: 88 34 5f b0 7c 36 a6 32 50 fb 9c 1f 36 84 86 6c
all: f4 aa fe e5 e3 0b c9 9e 56 b5 05 30 f4 27 80 3f

confsync checksum
global: 09 28 1a fd 1b 4c 7d 39 1b 67 8a 62 e0 04 f8 b3
root: 8c 54 95 74 40 68 2c a7 3e ef e6 26 d3 37 09 08
mgmt-vdom: 88 34 5f b0 7c 36 a6 32 50 fb 9c 1f 36 84 86 6c
all: f4 aa fe e5 e3 0b c9 9e 56 b5 05 30 f4 27 80 3f
```

The example output includes four sets of checksums: a checksum for the global configuration, a checksum for each VDOM (in this case there are two VDOMs: root and mgmt-vdom), and a checksum for the complete configuration (all). You can verify that this FPM is synchronized because both sets of HA checksums match and both sets of confsync checksums match. Also as expected, the HA and confsync checksums are different.

If the FIMs and FPMs in a standalone FortiGate-7000E have the same set of checksums, the FIMs and FPMs in that FortiGate-7000E are synchronized.

If a FIM or FPM is out of sync, you can use the output of the `diagnose sys configsync status` command to determine what part of the configuration is out of sync. You could then take action to attempt to correct the problem or contact Fortinet Technical Support at https://support.fortinet.com for assistance.

A corrective action could be to restart of the component with the synchronization error. You could also try using the following command to re-calculate the checksums in case the sync error is just temporary:

```
diagnose sys confsync csum-recalculate
```

Multi VDOM mode

By default, when you first start up a FortiGate-7000E it is operating in Multi VDOM mode. The default Multi VDOM configuration includes the **root** VDOM and a management VDOM named **mgmt-vdom**. The management interface (mgmt) and the HA heartbeat interfaces (M1, M2) are in mgmt-vdom and all the data interfaces are in the root VDOM.

You cannot delete or rename mgmt-vdom. You also cannot remove interfaces from it or add interfaces to it. You can; however, configure other settings such as routing required for management communication, interface IP addresses, and so on. You can also add VLANs to the interfaces in mgmt-vdom.

You can use the root VDOM for data traffic and you can also add more VDOMs as required, depending on your Multi VDOM license.

Multi VDOM mode and HA

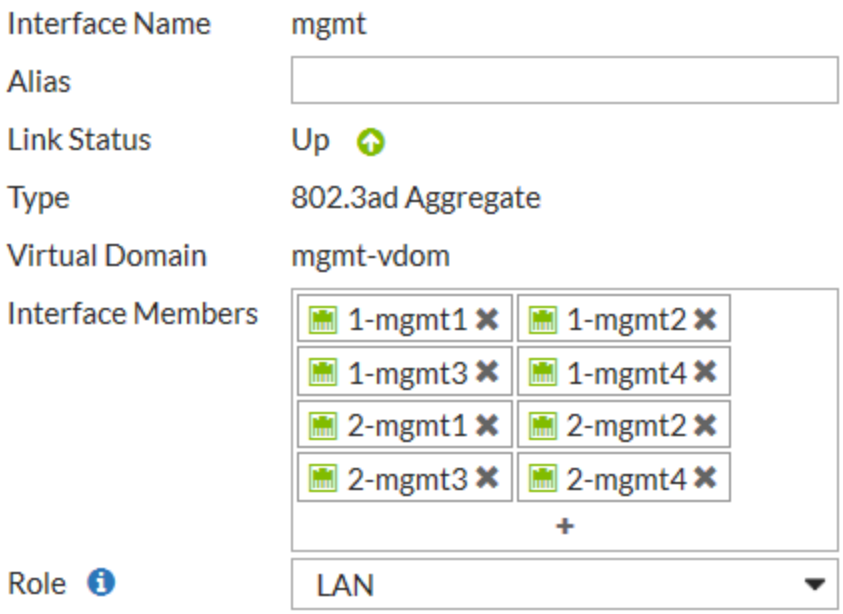
Multi VDOM mode supports all FortiGate-7000E HA configurations described in FortiGate-7000E high availability on page 68, including standard FGCP HA, virtual clustering, FGSP, standalone configuration synchronization, and VRRP.

To successfully form an FGCP HA cluster, both FortiGate-7000Es must be operating in the same VDOM mode (Multi or Split-Task). You should change both FortiGate-7000Es to the VDOM mode that you want them to operate in before configuring HA. To change the VDOM mode of an operating cluster, you need remove the backup FortiGate-7000E from the cluster, switch both FortiGate-7000Es to the other VDOM mode and then re-form the cluster. This process will cause traffic interruptions.

Setting up management connections

When your FortiGate-7060E 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



You can configure and manage your FortiGate-7060E 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. The default IP address is 192.168.1.99 and you can log in with the **admin** administrator account with no password.

For security reasons you should add a password to the admin account before connecting the chassis to your network.

Adding a password to the admin administrator account

For security purposes one of the first things you should do is add a password to the admin account.

Depending on your firmware version, when you first log into the GUI you maybe presented with an option to change the admin account password.

From the GUI, access the Global GUI and go to **System > Administrators**, edit the **admin** account, and select **Change Password**.

From the CLI:

```
config global
   config system admin
      edit admin
```

```
        set password <new-password>
    end
```

FortiGate-7000E 7.4.0 incompatibilities and limitations

FortiGate-7000E for FortiOS 7.4.0 has the following limitations and incompatibilities with FortiOS features:

The FortiGate-7000E uses the Fortinet Security Fabric for communication and synchronization between the FIMs and the FPMs and for normal GUI operation. By default, the Security Fabric is enabled and must remain enabled for normal operation.

Managing the FortiGate-7000E

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-7000E 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-7000E configuration includes a management VDOM named mgmt-vdom. For the FortiGate-7000E 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-7000E VDOMs.

Maximum number of LAGs and interfaces per LAG

The FortiGate-7000E supports 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. A FortiGate-7000E LAG can include up to 20 interfaces.

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 71

The following FortiOS HA features are not supported or are supported differently by the FortiGate-7000E:

- Active-active HA is not supported.
- The range for the HA `group-id` is 0 to 31.
- Failover logic for FortiGate-7000E HA is not the same as FGCP for other FortiGate clusters.
- HA heartbeat configuration is specific to FortiGate-7000E systems and differs from standard HA.
- FortiGate-7000E HA does not support the `route-wait` and `route-hold` options for tuning route synchronization between FortiGate-7000Es.
- VLAN monitoring using the `config system ha-monitor` command is not supported.
- FortiGate-7000E HA does not support using the HA session-sync-dev option. Instead, session synchronization traffic uses the M1 and M2 interfaces, separating session sync traffic from data traffic.

Shelf manager module

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

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

FortiOS features not supported by FortiGate-7000E

The following mainstream FortiOS features are not supported by the FortiGate-7000E:

See the FortiGate-6000 and 7000 platforms Known Issues section of the FortiOS 7.4.0 release notes for information about FortiOS features not supported by the FortiGate-7000E for FortiOS 7.4.0.

- Hardware switch.
- DLP archiving.
- 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-7000E platform only supports quarantining files to FortiAnalyzer.
- The FortiGate-7000E does not support configuring dedicated management interfaces using the `config system dedicated-mgmt` command or by enabling the `dedicated-to management` interface option. The purpose of the dedicated management interface feature is to add a routing table just for management connections. This functionality is supported by the FortiGate-7000E management VDOM (mgmt-vdom) that has its own routing table and contains all of the FortiGate-7000E management interfaces.

- The FortiOS `session-ttl` option `never` (which means no session timeout) is only supported if the `dp-load-distribution-method` is set to `src-dst-ip-sport-dport` (the default) or `src-dst-ip` and the firewall policy that accepts the session does not perform NAT. If any other load distribution method is used, or if NAT is enabled, the DP session timer will terminate the session according to the DP processor session timer. For more information about the `never` option, see No session timeout.
- Enabling the system settings option `tcp-session-without-syn` and configuring a firewall policy to accept sessions without syn packets allows FortiOS to add entries to its session table for sessions that do not include SYN packets. These sessions can only be load balanced by the DP processor if the `dp-load-distribution-method` is set to `src-dst-ip-sport-dport` (default) or `src-dst-ip`. If any other load distribution method is used, the sessions will be dropped. As well, the DP processor cannot load balance these sessions if they are accepted by a firewall policy with NAT enabled.
- The `source-ip` option for management services (for example, logging, SNMP, connecting to FortiSandbox) that use interfaces in the mgmt-vdom is not supported and has been removed from the CLI.
- The `config vpn ssl settings` option `tunnel-addr-assigned-method` has been removed from the CLI because this option is not compatible with FortiGate-6000 and 7000 load balancing.

IPsec VPN tunnels terminated by the FortiGate-7000E

For a list of FortiGate-7000E IPsec VPN features and limitations, see IPsec VPN load balancing on page 62.

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 and spam filtering queries

The FortiGate-7000E sends all FortiGuard web filtering and spam filtering rating queries through a management interface from the management VDOM.

Web filtering quotas

On a VDOM operating with the **Inspection Mode** set to **Proxy**, you can go to **Security Profiles > Web Filter** and set up **Category Usage Quotas**. Each FPM has its own quota, and the FortiGate-7000E applies quotas per FPM and not per the entire FortiGate-7000E system. This could result in quotas being exceeded if sessions for the same user are processed by different FPMs.

Log messages no longer include a slot field

FortiGate- 7000 log messages no longer include information in the slot field. Instead, slot information is now always contained in the message field.

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-7000E, make sure to run `execute ping` tests from the primary FPM CLI.

Displaying the process name associated with a process ID

You can use the following command to display the process name associated with a process ID (PID):

```
diagnose sys process nameof <pid>
```

Where `<pid>` is the process ID.

Managing individual FortiGate-7000E FIMs and FPMs

You can manage individual FIMs and FPMs using special port numbers or the `execute load-balance slot manage` command. You can also use the `execute ha manage` command to log in to the other FortiGate-7000E in an HA configuration.

Special management port numbers

In some cases, you may want to connect to individual FIMs or FPMs to view status information or perform a maintenance task such as installing firmware or performing a restart. You can connect to the GUI or CLI of individual FIMs or FPMs in a FortiGate-7000E using the SLBC management interface IP address with a special port number.

You use the following command to configure the SLBC management interface:

```
config global
   config load-balance setting
      set slbc-mgmt-intf <interface>
   end
```

Where <interface> becomes the SLBC management interface.

To enable using the special management port numbers to connect to individual FIMs and FPMs, the SLBC management interface must be connected to a network, have a valid IP address, and have management or administrative access enabled. To block access to the special management port numbers, disconnect the mgmt interface from a network, configure the SLBC management interface with an invalid IP address, or disable management or administrative access for the SLBC management interface.

You can connect to the GUI of CLI of individual FIMs or FPMs using the SLBC management interface IP address followed by a special port number. For example, if the SLBC management interface IP address is 192.168.1.99, to connect to the GUI of the FPM in slot 3, browse to:

`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 slot number (in this example, 03).

You can view the special HTTPS management port number for and log in to the GUI of an FIM or FPM from the Configuration Sync Monitor.

The following table lists the special port numbers to use to connect to each FortiGate-7000E slot using common management protocols.

You can't change the special management port numbers. Changing configurable management port numbers, for example the HTTPS management port (which you might change to support SSL VPN), does not affect the special management port numbers.

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 FIM or FPM you have logged into, the GUI header banner and the CLI prompt shows its hostname. The System Information dashboard widget also shows the host name and serial number. The CLI prompt also shows the slot address in the format `<hostname> [<slot address>] #`.

Logging in to different FIMs or FPMs allows you to use dashboard widgets, FortiView, or Monitor GUI pages to view the activity of that FIM or FPM. Even though you can log in to different modules, you can only make configuration changes from the primary FIM; which is usually the FIM in slot 1.

FortiGate-7000E special management port numbers (slot numbers in order as installed in the chassis)

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

HA mode special management port numbers

In HA mode, you use the same special port numbers to connect to FIMs and FPMs in chassis 1 (chassis ID = 1) and different special port numbers to connect to FIMs and FPMs in chassis 2 (chassis ID = 2):

FortiGate-7000E HA special management 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	8003	44303	2303	2203	16103
Ch1 slot 1	FIM01	8001	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	8025	44325	2325	2225	16125
Ch2 slot 3	FPM03	8023	44323	2323	2223	16123
Ch2 slot 1	FIM01	8021	44321	2321	2221	16121
Ch2 slot 2	FIM02	8022	44322	2322	2222	16122

Chassis and Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Ch2 slot 4	FPM04	8024	44324	2324	2224	16124
Ch2 slot 6	FPM06	8026	44326	2326	2226	16126

Managing individual FIMs and FPMs from the CLI

From any CLI, you can use the `execute load-balance slot manage <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.

`<slot>` is the slot number of the slot that you want to log in to.

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 individual FIM and FPM CLIs of the secondary FortiGate-7000E in an HA configuration

From the primary FIM of the primary FortiGate-7000E in an HA configuration, you can use the following command to log in to the primary FIM of the secondary FortiGate-7000E:

```
execute ha manage <id>
```

Where `<id>` is the ID of the other FortiGate-7000E in the cluster. From the primary FortiGate-7000E, use an ID of 0 to log into the secondary FortiGate-7000E. From the secondary FortiGate-7000E, use an ID of 1 to log into the primary FortiGate-7000E. You can enter the ? to see the list of IDs that you can connect to.

After you have logged in, you can manage the secondary FortiGate-7000E from the primary FIM or you can use the `execute-load-balance slot manage` command to connect to the CLIs of the other FIM and the FPMs in the secondary FortiGate-7000E.

Load balancing and flow rules

This chapter provides an overview of how FortiGate-7000E Session-Aware Load Balancing (SLBC) works and then breaks down the details and explains why you might want to change some load balancing settings.

FortiGate-7000E SLBC works as follows.

1. The FortiGate-7000E directs all traffic that does not match a load balancing flow rule to the DP2 processors.

   If a session matches a flow rule, the session skips the DP2 processors and is directed according to the action setting of the flow rule. Default flow rules send traffic that can't be load balanced to the primary FPM. See Default configuration for traffic that cannot be load balanced on page 151.
2. The DP2 processors load balance TCP, UDP, SCTP, and IPv4 ICMP sessions among the FPMs according to the load balancing method set by the `dp-load-distribution-method` option of the `config load-balance setting` command.

   The DP2 processors load balance ICMP sessions among FPMs according to the load balancing method set by the `dp-icmp-distribution-method` option of the `config load-balance setting` command. See ICMP load balancing on page 52.

   The DP2 processors load balance GTP-U sessions if GTP load balancing is enabled. If GTP load balancing is disabled, the DP2 processors send GTP sessions to the primary FPM. For more information about GTP load balancing, see Enabling GTP load balancing on page 49.

   The DP2 processors load balance PFCP-controlled GTP-U sessions if PFCP load balancing is enabled. If PFCP load balancing is disabled, the DP2 processors send PFCP-controlled GTP-U sessions to the primary FPM. For more information about PFCP load balancing, see PFCP load balancing on page 51.

   To support ECMP you can change how the DP2 processors manage session tables, see ECMP support on page 111.
3. The DP2 processors send other sessions that cannot be load balanced to the primary FPM.

Setting the load balancing method

Sessions are load balanced or distributed by the DP2 processor 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 144.

Determining the primary FPM

You can determine which FPM is operating as the primary FPM by using the `diagnose load-balance status` command.

The following example `diagnose load-balance status` output for a FortiGate-7060E showing that the FPM in slot 3 is the primary 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
  Primary 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."
     Slot  5: FPM20E3E17900152
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  6: FPM20E3E17900202
       Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
```

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 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 load-balance flow-rule` command. The default configuration uses this command to send Kerberos, BGP, RIP, IPv4 and IPv6 DHCP, PPTP, BFD, IPv4 and IPv6 multicast, GTP, and HTTP and HTTPS authd sessions to the primary FPM. The default configuration also sends VRRP traffic to all FPMs. You can view the default configuration of the `config load-balance flow-rule` command to see how this is all configured, or see Default configuration for traffic that cannot be load balanced on page 151.

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
```

GTP load balancing

You can use the information in this section to optimize FortiGate-7000E GTP performance.

Enabling GTP load balancing

You can use the following load balancing command to enable or disable FortiGate-7000E GTP-U load balancing.

```
config load-balance setting
   config gtp-load-balance {disable | enable}
end
```

The following flow rule is also available to direct GTP-C traffic to the primary FPM.

```
config load-balance flow-rule
   edit 17
   set status disable
   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 primary blade"
   next
end
```

The recommended configuration for optimal GTP-C tunnel setup and GTP-U throughput performance is to enable `gtp-load-balance` and disable the GTP-C flow rule. In this configuration, both GTP-C and GTP-U traffic is load balanced among all of the FPMs:

```
config load-balance setting
   config gtp-load-balance enable
end
config load-balance flow-rule
   edit 17
   set status disable
   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 primary blade"
   next
end
```

If you want GTP-C traffic to only be processed by the primary FPM, you can edit the GTP-C 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 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 primary blade"
   next
end
```

GTP-U load balancing may not distribute sessions evenly among all of the FPMs. Its common in many 4G networks to have just a few SGWs. Similar configurations with very few servers may also be used in other GTP implementations. If the FortiGate-7000E receives GTP traffic from a very few servers, the GTP traffic will have very few source and destination IP addresses and TCP/IP ports. Since SLBC load balancing is based on source and destination IP addresses and TCP ports, its possible that sessions will not be distributed evenly among the FPMs. In fact, most GTP-U traffic could be processed by a limited number of FPMs.

Enabling GTP-U load balancing still distributes sessions and improves performance, but performance gains from enabling GTP-U load balancing may not be as high as anticipated.

GTP load balancing and fabric channel usage

On a FortiGate-7000E, when GTP load balancing is enabled, GTP tunnels are synchronized over the fabric channel backplane (also called the data channel). The fabric channel is also used for SLBC session synchronization. On a busy FortiGate-7000E that is also load balancing GTP tunnels, the system may experience more lost SLBC heartbeats than normal.

To avoid missed heartbeats, you should increase the `max-miss-heartbeats` load balancing setting.

For example, when GTP load balancing is enabled, Fortinet recommends setting the `max-miss-heartbeats` to 40.

```
config load-balance setting
   set max-miss-heartbeats 40
   set gtp-load-balance enable
end
```

Optimizing FortiOS Carrier NPU GTP performance

If your FortiGate-7000E is licensed for FortiOS Carrier, You can use the following command to optimize GTP performance:

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

There are independent Receive and Transmit queues for GTP-U processes. These queues and their associated resources are initialized when `gtp-enhance-mode` is enabled. After entering this command you should restart your FortiGate-7000E to initialize the changes.

If you restore a configuration file, and if that restored configuration file has a different `gtp-enhance-mode` setting you should restart your FortiGate-7000E to initialize the changes.

You can also use the following command to select the CPUs that can perform GTP-U packet inspection.

```
config system npu
   set gtp-enhance-cpu-range {0 | 1 | 2}
end
```

Where:

`0` all CPUs will process GTP-U packets

`1` only primary CPUs will process GTP-U packets.

`2` only secondary CPUs will process GTP-U packets.

PFCP load balancing

FortiGate-7000E includes support for load balancing the Packet Forwarding Control Protocol (PFCP). PFCP is a new addition to 3GPP that provides 4G Control plane and User Plane Separation (CUPS) and 5G signaling evolution. When PFCP is used as the control plane, the user plane employs GTP-U encapsulation. PFCP takes many of the roles that are provided by GTP-C in 3G/4G networks today and provides session awareness and tracking of GTP-U user plane traffic while also providing control plane initiation.

FortiGate-7000E PFCP support includes supporting PFCP session synchronization for FGCP HA.

You can use the following command to enable or disable FortiGate-7000E PFCP load balancing.

```
config load-balance setting
   set pfcp-load-balance {disable | enable}
end
```

The following flow rule is also available to direct PFCP control plane traffic to the primary FPM.

```
edit 21
   set status disable
   set vlan 0
   set ether-type ipv4
   set src-addr-ipv4 0.0.0.0 0.0.0.0
   set dst-addr-ipv4 0.0.0.0 0.0.0.0
   set protocol udp
   set src-l4port 0-0
   set dst-l4port 8805-8805
   set action forward
   set forward-slot master
   set priority 5
   set comment "pfcp to primary blade"
end
```

By default, both of these configurations are disabled and PFCP control plane and user plane traffic is not load balanced. The DP sends all PFCP control plane and user plane traffic to the primary FPM.

To load balance PFCP user plane traffic to multiple FPMs, you can set `pfcp-load-balance` to `enable`. This also enables the PFCP flow rule. PFCP user plane traffic is then load balanced across all FPMs while PFCP control plane traffic is still handled by the primary FPM. This is the recommended configuration for load balancing PFCP traffic.

These options are also available if your FortiGate-7000E is licensed for FortiOS Carrier. For more information about PFCP and FortiOS Carrier, see FortiOS Carrier PFCP protection.

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 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.

Load balancing TCP, UDP, and ICMP sessions with fragmented packets

If your FortiGate-7000E receives fragmented TCP, UDP, or ICMP packets, use the following command to make sure the Internal Switch Fabric (ISF) handles them correctly.

```
config load-balance setting
   set sw-load-distribution-method src-dst-ip
end
```

If `sw-load-distribution-method` is set to `src-dst-ip-sport-dport`, fragmented packets may be dropped.

When the DP2 processor receives a header fragment packet, if a matching session is found, the DP2 processor creates an additional fragment session matching the source-ip, destination-ip, and IP identifier (IPID) of the header fragment packet. Subsequent non-header fragments will match this fragment session and be forwarded to the same FPM as the header fragment.

You can use the following configuration to enable or disable this method of handling TCP, UDP, and ICMP sessions with fragmented packets.

```
config load-balance setting
   set dp-fragment-session enable
end
```

If you disable `dp-fragment-session`, handling fragmented packets is less efficient because the DP2 processor broadcasts all non-header fragmented TCP, UDP, or ICMP packets to all FPMs. FPMs that also received the header fragments of these packets re-assemble the packets correctly. FPMs that did not receive the header fragments discard the non-header fragments.

The age of the fragment session can be controlled using the following command:

```
config system global
   set dp-fragment-timer <timer>
end
```

The default `<timer>` value is 120 seconds. The range is 1 to 65535 seconds.

Adding flow rules to support DHCP relay

The FortiGate-7000E 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-7000E you must add a flow rule similar to the following to support port 67 DHCP traffic in both directions (the following example uses `edit 0` to add the DHCP relay flow using the next available flow rule index number):

```
config load-balance flow-rule
  edit 0
    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
```

The default configuration also includes the following flow rules for IPv6 DHCP traffic:

```
   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
```

These flow rules handle traffic when the IPv6 DHCP client sends requests to a DHCP server using port 547 and the DHCP server responds using port 546. 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 547. If this DHCP relay traffic passes through the FortiGate-7000E you must add a flow rule similar to the following to support port 547 DHCP traffic in both directions (the following example uses `edit 0` to add the DHCP relay flow using the next available flow rule index number):

```
config load-balance flow-rule
   edit 0
      set status enable
      set vlan 0
      set ether-type ipv6
      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 547-547
      set dst-l4port 547-547
      set action forward
      set forward-slot master
      set priority 5
      set comment "dhcpv6 relay"
   next
```

Flow rules to support multihop BFD (MBFD)

The FortiGate-7000E supports Multihop BFD for normal traffic and over IPsec VPN tunnels that are terminated by the FortiGate-7000E (see BFD for multihop path for BGP).

The multihop control protocol uses TCP and UDP traffic on port 4784. Multihop control traffic is not load balanced by DP processors. Instead, a flow rule is used to send all multihop control traffic to a single FPM.

The following flow rule has been added to the default flow rules for traffic that cannot be load balanced to send all multihop control traffic to the primary FPM. This flow rule should be enabled if you configure multihop BFD support on your FortiGate-7000E.

```
config load-balance flow-rule
   edit 22
      set status disable
      set vlan 0
      set ether-type ip
      set protocol udp
      set src-l4port 0-0
      set dst-l4port 4784-4784
```

```
      set action forward
      set forward-slot master
      set priority 5
      set comment "Flow Rule for Multihop BFD"
   end
```

Flow rules to support IP multicast

IPv4 and IPv6 Multicast traffic cannot be load balanced by DP processors and instead is sent to the primary FPM. This is controlled by the following default flow rules:

```
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
```

Controlling SNAT port partitioning behavior

You can use the following command to control how the FortiGate-7000E partitions source NAT (SNAT) source ports among FPMs:

```
config load-balance setting
   set nat-source-port {chassis-slots | enabled-slots}
end
```

`chassis-slots` this option statically allocates SNAT source ports to all FPMs that are enabled when you enter the command. If you disable an FPM from the CLI or remove an FPM from its slot, the SNAT source ports assigned to that FPM will not be re-allocated to the remaining FPMs. All FPMs that are still operating will maintain the same SNAT source port allocation and active sessions being processed by the still operating FPMs will not be affected.

You can use the following command to enable or disable an FPM from the CLI:

```
config workers
   edit <slot>
      set status {disable | enable}
   end
```

`enabled-slots` this option dynamically re-distributes SNAT source ports to enabled or installed FPMs. This is the default behavior and is recommended in most cases.

If an FPM is disabled or removed from its slot, SLBC dynamically re-allocates SNAT source ports among the remaining FPMs. This means that all configured SNAT source ports remain available. If SNAT source ports are re-allocated when the FortiGate-7000E is actively processing traffic, some active sessions may be lost if their source ports are allocated to different FPMs.

SNAT source ports are not dynamically reallocated if an FPM is powered off. To re-allocate SNAT source ports, the FPM must be disabled from the CLI or physically removed from its slot.

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.

Maximum number of flow rules limited by hardware

For all FortiGate-7000E models, the CLI allows you to add up to 512 flow rules. This number of flow rules is also supported the FortiGate-7000E internal switch hardware.

SSL VPN load balancing

FortiGate-7000E supports load balancing SSL VPN tunnel mode sessions terminated by the FortiGate-7000E. By default SSL VPN load balancing is disabled and a flow rule is required to send all SSL VPN sessions to one FPM (usually the primary FPM).

To support SSL VPN tunnel load balancing, you must disable all flow rules that match the SSL VPN traffic to be load balanced.

For SSL VPN load balancing to work properly, the DP processor load distribution method must be changed to a setting that does not include `src-port`. The following DP load distribution methods are supported for SSL VPN load balancing:

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

Then you can use the following command to enable SSL VPN load balancing:

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

When you enable SSL VPN load balancing, the FortiGate-7000E restarts SSL VPN processes running on the FIMs and the FPMs, resetting all current SSL VPN sessions. This restart will interrupt any active SSL VPN sessions.

Once the SSL VPN processes restart, the FortiGate-7000E DP2 processor distributes SSL VPN tunnel mode sessions to all of the FPMs.

To be able to distribute SSL VPN sessions to all FPMs, SSL VPN load balancing statically allocates the IP addresses in SSL VPN IP pools among the FPMs. Each FPM acquires a subset of the IP addresses in the IP pool. You may need to expand the number of IP addresses in your SSL VPN IP pools to make sure enough IP addresses are available for each FPM.

SSL VPN IP pool IP addresses are not re-allocated if an FPM goes down, is disabled, or is taken offline. The IP pool IP addresses assigned to the missing FPM are not available until the FPM returns to normal operation.

No other special configuration is required to support SSL VPN tunnel mode load balancing.

For more information on FortiGate-7000E SSL VPN load balancing, see this Fortinet Community article:Technical Tip : How to load balance SSL VPN web-mode traffic on FortiGate-6000 series.

Setting up SSL VPN using flow rules

As an alternative to SSL VPN load balancing, you can manually add SSL VPN load balancing flow rules to configure the FortiGate-7000E to send all SSL VPN sessions to the primary FPM. To match SSL VPN traffic, the flow rule should include a destination port that matches the destination port of the SSL VPN server. A basic rule to send SSL VPN traffic to the primary FPM could be:

```
config load-balance flow-rule
```

```
edit 0
   set status enable
   set ether-type ipv4
   set protocol tcp
   set dst-l4port 443-443
   set forward-slot master
   set comment "ssl vpn server to primary worker"
end
```

This flow rule matches all sessions sent to port 443 (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 (443). This flow rule also matches all other sessions using 443 as the destination port so all of this traffic is also sent to the primary FPM.

As a best practice, if you add a flow rule for SSL VPN, Fortinet recommends using a custom SSL VPN port (for example, 10443 instead of 443). This can improve performance by allowing SSL traffic on port 443 that is not part of your SSL VPN to be load balanced to FPMs instead of being sent to the primary FPM by the SSL VPN flow rule.

If you change the SSL VPN server listening port

If you have changed the SSL VPN server listening port to 10443, you can change the SSL VPN flow rule as follows:

```
config load-balance flow-rule
   edit 26
      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 worker"
   end
```

You can also make the SSL VPN flow rule more specific by including the SSL VPN server interface in the flow rule. For example, if your FortiGate-7000E listens for SSL VPN sessions on the 1-B4 interface:

```
config load-balance flow-rule
   edit 26
      set status enable
      set ether-type ipv4
      set protocol tcp
      set src-interface 1-B4
      set dst-l4port 10443-10443
      set forward-slot master
      set comment "ssl vpn server to primary worker"
   end
```

Adding the SSL VPN server IP address

You can also add the IP address of the FortiGate-7000E interface that receives SSL VPN traffic to the SSL VPN flow rule to make sure that the flow rule only matches the traffic of SSL VPN clients connecting to the SSL VPN server. For example, if the IP address of the interface is 172.25.176.32:

```
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 worker"
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.

IPsec VPN load balancing

The FortiGate-7000E uses SLBC load balancing to select an FPM to terminate traffic for a new IPsec VPN tunnel instance and all traffic for that tunnel instance is terminated on the same FPM.

```
config vpn ipsec phase1-interface
   edit <name>
      set ipsec-tunnel-slot {auto | FPM3 | ... | FPMX | master}
   end
```

You can optionally use the IPsec tunnel phase 1 configuration to select a specific FPM to terminate all tunnel instances started by that phase 1. For example, to terminate all tunnels on FPM4:

```
config vpn ipsec phase1-interface
   edit <name>
      set ipsec-tunnel-slot FPM4
   end
```

FortiGate-7000E IPsec VPN supports the following features:

- Interface-based IPsec VPN (also called route-based IPsec VPN).
- Site-to-Site IPsec VPN.
- Dialup IPsec VPN. The FortiGate-7000E can be the dialup server or client.
- Static and dynamic routing (BGP, OSPF, and RIP) over IPsec VPN tunnels.
- When an IPsec VPN tunnel is initialized, the SA is synchronized to all FPMs in the FortiGate-7000E, or in both FortiGate-7000Es in an HA configuration.
- Traffic between IPsec VPN tunnels is supported when both tunnels terminate on the same FPM.
- When setting up a VRF configuration to send traffic between two IPsec VPN interfaces with different VRFs, both IPsec tunnels must terminate on the same FPM.

FortiGate-7000E IPsec VPN has the following limitations:

- Policy-based IPsec VPN tunnels terminated by the FortiGate-7000E are not supported.
- Policy routes cannot be used for communication over IPsec VPN tunnels.
- IPv6 clear text traffic over IPv4 or IPv6 IPsec tunnels terminated on the FortiGate-7000E is not supported. This limitation does not affect IPv4 clear text traffic over IPv4 or IPv6 IPsec tunnels terminated on the FortiGate-7000E. This limitation also does not affect any pass through IPsec tunnel traffic that does not terminate on the FortiGate-7000E.
- IPsec SA synchronization between FGSP HA peers is not supported.
- When setting up an IPsec VPN VLAN interface, do not set the VLAN ID to 1. This VLAN ID is reserved by FortiOS. Any configurations that use a VLAN with VLAN ID = 1 will not work as expected.
- The FortiGate-7000E, because it uses DP processors for SLBC, does not support IPsec VPN to remote networks with 0- to 15-bit netmasks.
- UDP-encapsulated ESP (UESP) sessions that use the normal IKE port (port 4500) are load balanced by the DP2 processor in the same way as normal IPSec traffic. You can use the `ipsec-tunnel-slot` option when creating a phase 1 configuration to control how UESP tunnels are load balanced. However, if UESP sessions use a custom IKE port, the DP2 processor does not handle them as IPsec packets. Instead , they are load balanced by the DP2 processor in the same way as any other traffic. If required, you can adjust load balance settings or add a flow rule for UESP sessions using a custom IKE port.

Configuring IPsec VPN load balancing

Since the FortiGate-7000E 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 IPsec VPN load balancing sends all IPsec VPN sessions to the primary FPM.

Example IPv4 and IPv6 IPsec VPN flow rules

You can optionally add your own flow rules if you want to handle IPsec VPN sessions differently, for example, you could send IPsec VPN traffic to a different FPM instead of the primary FPM.

The following example IPv4 and IPv6 IPsec VPN flow rules send all IPv4 and IPv6 IPSec VPN traffic to the primary FPM. Normally you would not need these flow rules because IPsec VPN load balancing is disabled and all IPsec VPN traffic is just sent to the primary FPM.

```
 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
```

SD-WAN with multiple IPsec VPN tunnels

To support SD-WAN with IPsec VPN, the IPsec VPN tunnel configuration of all IPsec VPN tunnels that are members of the same SD-WAN zone in the same VDOM must send traffic to the same FPM. This means the `ipsec-tunnel-slot`

configuration of the IPsec VPN tunnel must include a specific FPM. Setting `ipsec-tunnel-slot` to `master` is not recommended, since the primary FPM can change. Setting `ipsec-tunnel-slot` to `auto` is not supported.

Please note the following limitations for this feature:

- Auto negotiation must be enabled in the IPsec VPN phase 2 configuration for all IPsec tunnels added to an SD-WAN zone.
- An SD-WAN zone can include a mixture of IPsec VPN interfaces and other interface types (for example, physical interfaces). If an SD-WAN zone contains an IPsec VPN interface, all traffic accepted by interfaces in that SD-WAN zone is sent to the same FPM, including traffic accepted by other interface types.
- SD-WAN health checking is not supported for IPsec VPN SD-WAN members.
- SD- WAN traffic information, including packet statistics, policy hit counts, and so on is not supported for IPsec VPN SD-WAN members.

Example FortiGate-7000E IPsec VPN VRF configuration

The following shows the basics of how to set up a VRF configuration that allows traffic between two IPsec VPN interfaces with different VRFs on a FortiGate-7000E. To support this configuration, both IPsec tunnels must terminate on the same FPM, in this example, the FPM in slot 5.

Create two VLAN interfaces:

```
config system interface
   edit "v0031"
      set vdom "vrf1"
      set vrf 10
      set ip <ip-address>
      set interface "port1"
      set vlanid 31
   next
   edit "v0032"
      set vdom "vrf1"
      set vrf 11
      set ip <ip-address>
      set interface "port2"
      set vlanid 32
   next
```

Create two phase1-interface tunnels. Add each tunnel to one of the VLAN interfaces created in step 1. The `ipsec-tunnel-slot` setting for both is `FPM5`.

```
config vpn ipsec phase1-interface
   edit "p1-v31"
      set interface "v0031"
      set local-gw <ip-address>
      set peertype any
      set proposal 3des-sha256
      set remote-gw <ip-address>
      set psksecret <psk>
      set ipsec-tunnel-slot FPM5
   next
      edit "p1-v32"
      set interface "v0032"
      set local-gw <ip-address>
```

```
      set peertype any
      set proposal 3des-sha256
      set remote-gw <ip-address>
      set psksecret <psk>
      set ipsec-tunnel-slot FPM5
   end
```

Edit each IPsec VPN interface and set the VRF ID for each one:

```
config system interface
   edit "p1-v31"
      set vdom "vrf1"
      set vrf 10
      set type tunnel
      set interface "v0031"
   next
   edit "p1-v32"
      set vdom "vrf1"
      set vrf 11
      set type tunnel
      set interface "v0032"
   end
```

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-7000E HA, run this command from the primary FortiGate-7000E. The third line of the command output shows which FPM is operating as the primary FPM.

```
diagnose load-balance status
  FIM01: FIM04E3E16000074
  Primary 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
  Primary 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-7000E high availability

FortiGate-7000E for FortiOS 6.4 supports the following types of HA operation:

- FortiGate Clustering protocol (FGCP)
- Virtual clustering (Virtual clustering on page 86)
- FortiGate Session Life Support Protocol (FGSP) (FortiGate-7000E FGSP on page 98)
- Standalone configuration synchronization (Standalone configuration synchronization on page 107)
- Virtual Router Redundancy Protocol (VRRP) (FortiGate-7000E VRRP HA on page 109)

Introduction to FortiGate-7000E FGCP HA

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

In Multi VDOM mode, virtual clustering is supported. Virtual clustering is not supported in Split-Task VDOM mode. Split-Task VDOM mode supports standard FGCP HA.

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 71. 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.

To successfully form an FGCP HA cluster, both FortiGate-7000Es must be operating in the same VDOM mode (Multi or Split-Task). You can change the VDOM mode after the cluster has formed, but this will disrupt traffic.

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

If both FortiGate-7000Es in a cluster are configured with the same chassis ID, both chassis begin operating in HA mode without forming a cluster. A message similar to the following is displayed on the CLI console of both devices:

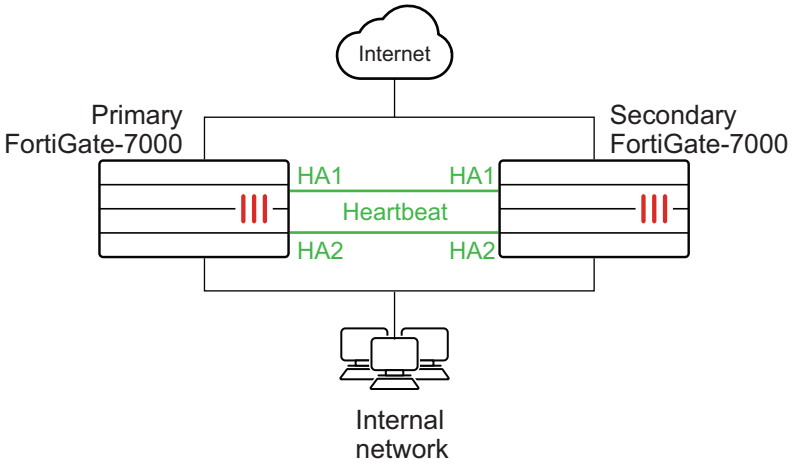
```
HA cannot be formed because this box's chassis-id 1 is the same from the
HA peer 'F76E9D3E17000001' chassis-id 1.
```

As well, a log message similar to the following is created:

```
Jan 29 16:29:46 10.160.45.70 date=2020-01-29 time=16:29:51 devname="CH-
02" devid="F76E9D3E17000001" slot=1 logid="0108037904" type="event"
subtype="ha" level="error" vd="mgmt-vdom" eventtime=1580344192162305962
tz="-0800" logdesc="Device set as HA primary" msg="HA group detected
chassis-id conflict" ha_group=7 sn="F76E9DT018900001 chassis-id=1"
```

You can resolve this issue by logging into one of the FortiGates and changing its Chassis ID to 2. When this happens, the two chassis will form a cluster.

Example FortiGate-7040 HA configuration



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

Before you begin configuring HA

Before you begin:

- The FortiGate-7000Es must be running the same FortiOS firmware version
- The FortiGate-7000Es must be in the same VDOM mode (Multi VDOM or Split-Task VDOM mode).
- To successfully form an FGCP HA cluster, both FortiGate-7000Es must be operating in the same VDOM mode (Multi or Split-Task). You should change both FortiGate-7000Es to the VDOM mode that you want them to operate in before configuring HA. To change the VDOM mode of an operating cluster, you need remove the backup

FortiGate-7000E from the cluster, switch both FortiGate-7000Es to the other VDOM mode and then re-form the cluster. This process will cause traffic interruptions.

- Interfaces should be configured with static IP addresses (not DHCP or PPPoE).
- Register and apply licenses to each FortiGate-7000E 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-7000Es 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 interfaces before configuring HA

You should configure split interfaces or change interfaces types on both FortiGate-7000Es before forming an FGCP HA cluster. If you decide to change the split interfaces or interface type configuration after forming a cluster, you need to remove the backup FortiGate-7000E from the cluster and change interface configuration on both FortiGate-7000Es separately. After the FortiGate-7000Es restart, you can re-form the cluster. This process will cause traffic interruptions.

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-7000E reboots and synchronizes the configuration.

On each FortiGate-7000E, 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, Secondary, uptime=58852.50, priority=2, slot_id=2:2, idx=3, flag=0x10, in_sync=1
FIM04E3E16000010, Secondary, uptime=58726.83, priority=3, slot_id=1:1, idx=0, flag=0x10, in_sync=1
FIM04E3E16000014, Primary, uptime=58895.30, priority=1, slot_id=2:1, idx=1, flag=0x10, in_sync=1
FIM10E3E16000040, Secondary, uptime=58857.80, priority=4, slot_id=1:2, idx=2, flag=0x10, in_sync=1
FPM20E3E16900234, Secondary, uptime=58895.00, priority=16, slot_id=2:3, idx=4, flag=0x64, in_sync=1
FPM20E3E16900269, Secondary, uptime=58333.37, priority=120, slot_id=2:4, idx=5, flag=0x64, in_sync=1
FPM20E3E17900113, Secondary, uptime=58858.90, priority=116, slot_id=1:3, idx=6, flag=0x64, in_sync=1
FPM20E3E17900217, Secondary, 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-7000Es 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.

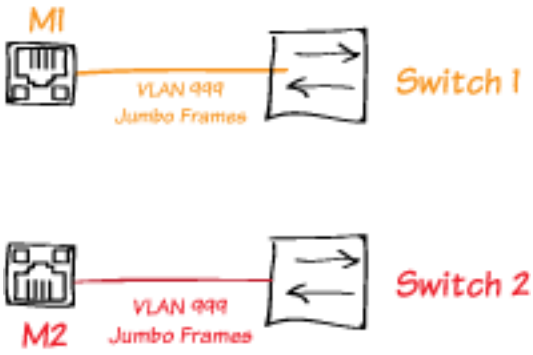
All of the M1 interfaces must be connected together with a switch and all of the M2 interfaces must be connected together with another switch. Connecting M1 interfaces or M2 interfaces directly is not supported as each FIM needs to communicate with all other FIMs.

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.

For redundancy, for other FortiGate-7000Es, 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. You must also configure switches used for HA heartbeat traffic in trunk mode.

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.

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.



Default HA heartbeat VLAN triple-tagging

By default, HA heartbeat packets are VLAN packets with VLAN ID 999, an outer TPID of 0x8100, an ethertype of 8890, and an MTU value of 1500. The default proprietary HA heartbeat VLAN tagging uses the following triple tagging format:

```
TPID 0x8100 VLAN <vlan-id> (by default 999) + TPID 0x88a8 VLAN 10/30 + TPID 0x8100 VLAN
10/30 + ethernet packet
```

If your switch is compatible with Fortinet's proprietary triple-tagging format then all you need to do is use the following options to give the M1 and M2 interfaces different VLAN tags.

```
config system ha
   set ha-port-dtag-mode proprietary
   set hbdev-vlan-id <vlan>
```

```
   set hbdev-second-vlan-id <vlan>
end
```

Where:

- `ha-port-dtag-mode` is set to `proprietary` and the FortiGate-7000E uses the default triple-tagging format.
- `hbdev-vlan-id` sets the outer VLAN ID used by M1 interface heartbeat packets.
- `hbdev-second-vlan-id` sets the outer VLAN ID used by M2 interface heartbeat packets. The M1 and M2 interfaces must have different outer VLAN IDs if they are connected to the same switch.

If your switch is not compatible with Fortinet's proprietary triple-tagging format, you can use the following options to change the outer TPID and ethertype.

```
config system ha
   set ha-port-dtag-mode proprietary
   set ha-port-outer-tpid {0x8100 | 0x88a8 | 0x9100}
   set ha-eth-type <ethertype>
end
```

Where:

- `ha-port-dtag-mode` is set to `proprietary` and the FortiGate-7000E uses the default triple-tagging format.
- `ha-port-outer-tipd` sets the outer TPID to be compatible with the switch. The default outer TPID of `0x8100`, is compatible with most third-party switches.
- `ha-eth-type` sets the HA heartbeat packet ethertype (default 8890) to be compatible with the switch.

If your switch doesn't support triple tagging, see HA heartbeat VLAN double-tagging on page 73.

Example triple-tagging compatible switch configuration

The switch that you use for connecting HA heartbeat interfaces does not have to support IEEE 802.1ad (also known as Q-in-Q, double-tagging), but the switch should be able to forward the double-tagged frames. Fortinet recommends avoiding switches that strip out the inner tag. 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-7000E 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-7000Es 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 ha-port-dtag-mode proprietary
   ```

```
    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` or `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
```

HA heartbeat VLAN double-tagging

FortiGate-7000E HA supports HA heartbeat double-tagging to be compatible with third-party switches that do not support Fortinet's proprietary triple tagging format. HA heartbeat double-tagging has the following format:

```
TPID 0x8100 VLAN <vlan-id> (by default 999) + TPID 0x8100 VLAN 10/30 + ethernet packet
```

You can use the following commands to set the HA VLAN tagging mode to double-tagging, customize the outer TPID, and set the VLAN IDs for M1 and M2. Both FortiGates in the cluster must have the same VLAN tagging configuration.

```
config system ha
   set ha-port-dtag-mode double-tagging
   set ha-port-outer-tpid {0x8100 | 0x88a8 | 0x9100}
   set hbdev-vlan-id <vlan>
   set hbdev-second-vlan-id <vlan>
```

```
   set ha-eth-type <ethertype>
end
```

Where:

`ha-port-dtag-mode` is set to `double-tagging` and the FortiGate-7000E uses the double-tagging format.

`ha-port-outer-tipd` sets the outer TPID to be compatible with the switch. The default outer TPID of `0x8100` is compatible with most third-party switches.

`hbdev-vlan-id` sets the outer VLAN ID used by M1 interface heartbeat packets.

`hbdev-second-vlan-id` sets the outer VLAN ID used by M2 interface heartbeat packets. The M1 and M2 interfaces must have different outer VLAN IDs if they are connected to the same switch.

`ha-eth-type` sets the HA heartbeat packet ethertype (default 8890) to be compatible with the switch.

Example double-tagging switch configuration

The following switch configuration is compatible with FortiGate-7040E HA heartbeat double tagging and with the default TPID of `0x8100`.

The FortiGate-7040E HA heartbeat configuration is.

```
config system ha
   set ha-port-dtag-mode double-tagging
   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
```

Example third-party switch configuration:

Switch interfaces 37 to 40 connect to the M1 interfaces of the FIMs in both FortiGate-7040E chassis.

```
interface Ethernet37
description **** FGT-7000E M1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4086
switchport mode dot1q-tunnel
!
interface Ethernet38
description **** FGT-7000E M1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4086
switchport mode dot1q-tunnel
!
interface Ethernet39
description **** FGT-7000E M1 HA HB ****
speed forced 10000full
switchport access vlan 660
switchport trunk native vlan 4086
switchport mode dot1q-tunnel
!
interface Ethernet40
description **** FGT-7000E M1 HA HB ****
speed forced 10000full
switchport access vlan 660
```

```
switchport trunk native vlan 4086
switchport mode dot1q-tunnel
!
```

Switch interfaces 41 to 44 connect to the M2 interfaces of the FIMs in both FortiGate-7040E chassis.

```
interface Ethernet41
description **** FGT-7000E M2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4087
switchport mode dot1q-tunnel
!
interface Ethernet42
description **** FGT-7000E M2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4087
switchport mode dot1q-tunnel
!
interface Ethernet43
description **** FGT-7000E M2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4087
switchport mode dot1q-tunnel
!
interface Ethernet44
description **** FGT-7000E M2 HA HB ****
mtu 9214
speed forced 10000full
no error-correction encoding
switchport access vlan 770
switchport trunk native vlan 4087
switchport mode dot1q-tunnel
```

Basic FortiGate-7000E HA configuration

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

Make sure you give each FortiGate-7000E a different chassis ID. If both FortiGate-7000Es in a cluster are configured with the same chassis ID, both chassis begin operating in HA mode without forming a cluster. A message similar to the following is displayed on the CLI console of both devices:

```
HA cannot be formed because this box's chassis-id 1 is the same from the
HA peer 'F76E9D3E17000001' chassis-id 1.
```

As well, a log message similar to the following is created:

```
Jan 29 16:29:46 10.160.45.70 date=2020-01-29 time=16:29:51 devname="CH-
02" devid="F76E9D3E17000001" slot=1 logid="0108037904" type="event"
subtype="ha" level="error" vd="mgmt-vdom" eventtime=1580344192162305962
tz="-0800" logdesc="Device set as HA primary" msg="HA group detected
chassis-id conflict" ha_group=7 sn="F76E9DT018900001 chassis-id=1"
```

You can resolve this issue by logging into one of the FortiGate-7000Es and changing its Chassis ID to 2. When this happens, the two chassis will form a cluster.

1. Set up HA heartbeat communication as described in Connect the M1 and M2 interfaces for HA heartbeat communication on page 71.
2. Log into the GUI or CLI of the FIM in slot 1 of the FortiGate-7000E that will become chassis 1.
   Usually you would do this by connecting the management IP address of this FortiGate-7000E.
3. Use the following CLI command to change the host name. This step is optional, but setting a host name makes the FortiGate-7000E 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-7000E:
   ```
   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**, select the **Chassis identifier** (or chassis ID), and set the **Heartbeat Interface Priority** for the heartbeat interfaces (1-M1, 1-M2, 2-M1, and 2-M2). You must configure the group ID from the CLI.
5. Log into the chassis 2 FortiGate-7000E 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**, select the **Chassis identifier** (or chassis ID), and set the **Heartbeat Interface Priority** for the heartbeat interfaces (1-M1, 1-M2, 2-M1, and 2-M2). You must configure the group ID from the CLI.

Once you save your configuration changes, if the HA heartbeat interfaces are connected, the FortiGate-7000Es negotiate to establish a cluster. You may temporarily lose connectivity with the FortiGate-7000Es as the cluster negotiates and the FGCP changes the MAC addresses of the FortiGate-7000E 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 71.

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

The following example FortiGate-7000E `get system ha status` output shows a FortiGate-7000E cluster that is operating normally. The output shows which FortiGate-7000E has become the primary FortiGate-7000E 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
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
Primary selected using:
    <2019/01/14 16:26:30> FG74E83E16000016 is selected as the primary because it has more
active switch blade.
    <2019/01/14 16:26:12> FG74E83E16000016 is selected as the primary because it's the only
member in the cluster.
ses_pickup: disable
override: disable
Configuration Status:
       FG74E83E16000016(updated 3 seconds ago): in-sync
```

```
        FG74E83E16000016 chksum dump: 7c 74 ce 81 83 c0 54 c1 01 1d 4f a9 c9 fd 17 df
        FG74E83E16000015(updated 4 seconds ago): in-sync
        FG74E83E16000015 chksum dump: 7c 74 ce 81 83 c0 54 c1 01 1d 4f a9 c9 fd 17 df
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
Primary: 7K-Chassis-1    , FG74E83E16000016, cluster index = 0
Secondary: 7K-Chassis-2    , FG74E83E16000015, cluster index = 1
number of vcluster: 1
vcluster 1: work 10.101.11.20
Primary : FG74E83E16000016, operating cluster index = 0
Secondary : FG74E83E16000015, operating cluster index = 1
Chassis Status: (Local chassis ID: 2)
    Chassis ID 1: Secondary Chassis
        Slot ID 1: Primary Slot
        Slot ID 2: Secondary Slot
    Chassis ID 2: Primary Chassis
        Slot ID 1: Primary Slot
        Slot ID 2: Secondary Slot
```

Confirming that the FortiGate-7000E HA cluster is synchronized

After an HA cluster is up and running, you can use the HA Status dashboard widget to view status information about the cluster. You can also use the `get system ha status` command to confirm that the cluster is operating normally. As highlighted below, the command shows the HA health status, describes how the current primary FortiGate-7000E was selected, shows if the configuration is synchronized (configuration status), and indicates the serial numbers of the primary and secondary FortiGate-7000Es.

```
get system ha status
HA Health Status: OK
...
Primary selected using:
```

```
    <2019/09/23 12:56:53> FG74E43E17000073 is selected as the primary because it has the
largest value of override priority.
...

Configuration Status:
    FG74E17000073(updated 2 seconds ago): in-sync
    FG74E43E17000073 chksum dump: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2
    FG74E43E17000065(updated 4 seconds ago): in-sync
    FG74E43E17000065 chksum dump: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2
...
Primary: FG74E43E17000073, operating cluster index = 0
Secondary: FG74E43E17000065, operating cluster index = 1
```

For a FortiGate-7000E HA cluster to operate normally, the configurations of both FortiGate-7000Es and the FIMs and FPMs in these devices must be synchronized. The `Configuration Status` information provided by the `get system ha status` command is a useful indicator of synchronization status of the cluster. The information provided indicates whether the FortiGate-7000Es in the cluster are `in-sync` (or `out-of-sync`) and includes checksums of each FortiGate-7000E configuration. If the two FortiGate-7000Es are synchronized, these checksums must match.

Viewing more details about HA cluster synchronization

You can use the `diagnose sys ha checksum show` command to display the debugzone and configuration checksums for the FortiGate-7000E in the cluster that you have logged in to.

```
diagnose sys ha checksum show
is_manage_primary()=1, is_root_primary()=1
debugzone
global: 7e 06 79 02 65 a9 ea e3 68 58 73 c2 33 d0 16 f1
root: 43 2c ee 2c f1 b3 b2 13 ff 37 34 5e 86 11 dc bf
mgmt-vdom: 9c 7d 58 9f 81 4b b7 4e ed 2a c3 02 34 b4 7c 63
all: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2

checksum
global: 7e 06 79 02 65 a9 ea e3 68 58 73 c2 33 d0 16 f1
root: 43 2c ee 2c f1 b3 b2 13 ff 37 34 5e 86 11 dc bf
mgmt-vdom: 9c 7d 58 9f 81 4b b7 4e ed 2a c3 02 34 b4 7c 63
all: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2
```

The first line of this example output indicates that the command is displaying information for the primary FortiGate-7000E. This command output then shows debugzone and checksum information for the primary FIM. You can verify that the primary FIM is synchronized because both sets of checksums match.

Each set of checksums includes a checksum for the global configuration, for each VDOM (in this case there are two VDOMs: root and mgmt-vdom), and a checksum for the complete configuration (all).

You can use the `diagnose sys ha checksum cluster` command to display the debugzone and configuration checksums for both FortiGate-7000Es in the cluster. The command output also indicates which FortiGate-7000E is the primary (`is_manage_primary()=1`) and the secondary (`is_manage_primary()=0`). If the cluster is synchronized, both FortiGate-7000Es will have the same checksums.

```
diagnose sys ha checksum cluster

================== FG74E43E17000073 ==================

is_manage_primary()=1, is_root_primary()=1
```

```
debugzone
global: 7e 06 79 02 65 a9 ea e3 68 58 73 c2 33 d0 16 f1
root: 43 2c ee 2c f1 b3 b2 13 ff 37 34 5e 86 11 dc bf
mgmt-vdom: 9c 7d 58 9f 81 4b b7 4e ed 2a c3 02 34 b4 7c 63
all: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2

checksum
global: 7e 06 79 02 65 a9 ea e3 68 58 73 c2 33 d0 16 f1
root: 43 2c ee 2c f1 b3 b2 13 ff 37 34 5e 86 11 dc bf
mgmt-vdom: 9c 7d 58 9f 81 4b b7 4e ed 2a c3 02 34 b4 7c 63
all: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2

================== FG74E43E17000065 ==================

is_manage_primary()=0, is_root_primary()=0
debugzone
global: 7e 06 79 02 65 a9 ea e3 68 58 73 c2 33 d0 16 f1
root: 43 2c ee 2c f1 b3 b2 13 ff 37 34 5e 86 11 dc bf
mgmt-vdom: 9c 7d 58 9f 81 4b b7 4e ed 2a c3 02 34 b4 7c 63
all: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2

checksum
global: 7e 06 79 02 65 a9 ea e3 68 58 73 c2 33 d0 16 f1
root: 43 2c ee 2c f1 b3 b2 13 ff 37 34 5e 86 11 dc bf
mgmt-vdom: 9c 7d 58 9f 81 4b b7 4e ed 2a c3 02 34 b4 7c 63
all: 0b 16 f2 e4 e2 89 eb a1 bf 8f 15 9b e1 4e 3b f2
```

Finally, you can also log into the CLI of each FortiGate-7000E in the cluster and use the `diagnose sys confsync showcsum` command to confirm that the configurations of the FIMs and FPMs in each FortiGate-7000E are synchronized.

The output of the command will also show that the ha checksums are the same for both FortiGate-7000Es, but the confsync checksums are different. This occurs because some parts of the configuration are not synchronized by HA so each FortiGate-7000E will have a different configuration and different confsync checksums.

See Viewing more details about FortiGate-7000E synchronization on page 37 for details about the `diagnose sys confsync showcsum` command.

Primary FortiGate-7000E selection with override disabled (default)

FortiGate-7000E FGCP selects the primary FortiGate-7000E based on standard FGCP primary unit selection and also accounting for the number of failed FPMs. The selection sequence is:

- At least one active FPM
- Failed FIMs
- Failed monitored interfaces
- Failed FPMs
- Age
- Device priority
- Serial number

In most cases and with default settings, if everything is connected and operating normally, the FortiGate-7000E with the highest serial number becomes the primary FortiGate-7000E. You can set the device priority higher on one of the FortiGate-7000Es if you want it to become the primary FortiGate-7000E.

The selection sequence also shows that at least one FPM must be active for a FortiGate-7000E to be selected to be the primary. If at least one FPM is active on each FortiGate-7000E, the most important criteria is the number of operating FIMs, followed by the number of connected monitored interfaces, and followed by the number of failed FPMs. So if one or more FPMs fail, if both FIMs are operating and if monitored interfaces are not configured or no monitored interface has become disconnected, the primary FortiGate-7000E will be the one with the most active FPMs.

Primary FortiGate-7000E selection with override enabled

With override enabled, FortiGate-7000E FGCP selects the primary FortiGate-7000E based on standard FGCP primary unit selection with override enabled and also accounting for the number of failed FIMs and FPMs. The selection sequence is:

- At least one active FPM
- Failed FIMs
- Failed monitored interfaces
- Failed FPMs
- Device priority
- Age
- Serial number

Enabling override and adjusting the device priority means that the FortiGate-7000E with the highest device priority becomes the primary FortiGate-7000E as long as both FIMs are operating, monitored interfaces are not configured, no monitored interface has become disconnected, and both FortiGate-7000Es have the same number of failed FPMs. Enabling override causes the cluster to negotiate more often to make sure that the FortiGate-7000E with the highest device priority always becomes the primary FortiGate-7000E.

Failover protection

FortiGate-7000E HA supports failover protection to provide FortiOS services even when one of the FortiGate-7000Es encounters a problem that would result in partial or complete loss of connectivity or reduced performance for a standalone FortiGate-7000E. This failover protection provides a backup mechanism that can be used to reduce the risk of unexpected downtime, especially in a mission-critical environment.

To achieve failover protection in a FortiGate-7000E cluster, one of the FortiGate-7000Es functions as the primary, processing traffic and the other as the secondary, operating in an active stand-by mode. The cluster IP addresses and HA virtual MAC addresses are associated with the interfaces of the primary. All traffic directed at the cluster is actually sent to and processed by the primary.

While the cluster is functioning, the primary FortiGate-7000E functions as the FortiGate network security device for the networks that it is connected to. In addition, the primary FortiGate-7000E and the secondary FortiGate-7000E use the HA heartbeat to keep in constant communication. The secondary FortiGate-7000E reports its status to the primary FortiGate-7000E and receives and stores connection and state table updates from the primary FortiGate-7000E.

FortiGate-7000E HA supports four kinds of failover protection:

- Device failure protection automatically replaces a failed device and restarts traffic flow with minimal impact on the network.
- FIM failure protection makes sure that traffic is processed by the FortiGate-7000E with the most operating FIMs.
- Link failure protection maintains traffic flow if a link fails.
- FPM failure protection makes sure that traffic is processed by the FortiGate-7000E with the most operating FPMs.
- Session failure protection resumes communication sessions with minimal loss of data if a device, module, or link failure occurs.

Device failure

If the primary FortiGate-7000E encounters a problem that is severe enough to cause it to fail, the secondary FortiGate-7000E becomes new primary FortiGate-7000E. This occurs because the secondary FortiGate-7000E is constantly waiting to negotiate to become primary FortiGate-7000E. Only the heartbeat packets sent by the primary FortiGate-7000E keep the secondary FortiGate-7000E from becoming the primary FortiGate-7000E. Each received heartbeat packet resets a negotiation timer in the secondary FortiGate-7000E. If this timer is allowed to run out because the secondary FortiGate-7000E does not receive heartbeat packets from the primary FortiGate-7000E, the secondary FortiGate-7000E assumes that the primary FortiGate-7000E has failed and becomes the primary FortiGate-7000E.

The new primary FortiGate-7000E will have the same MAC and IP addresses as the former primary FortiGate-7000E. The new primary FortiGate-7000E then sends gratuitous ARP packets out all of its connected interfaces to inform attached switches to send traffic to the new primary FortiGate-7000E. Sessions then resume with the new primary FortiGate-7000E.

FIM failure

If one or more FIMs in the primary FortiGate-7000E fails, the cluster renegotiates and the FortiGate-7000E with the most operating FIMs becomes the primary FortiGate-7000E. An FIM failure can occur if the FIM shuts down due to a software crash or hardware problem, or if the FIM is manually shut down or even removed from the chassis.

After the primary FortiGate-7000E experiences an FIM failure, the FortiGate-7000E with the most operating FIMs becomes the new primary FortiGate-7000E. The new primary FortiGate-7000E sends gratuitous arp packets out all of its connected interfaces to inform attached switches to send traffic to it. Sessions then resume with the new primary FortiGate-7000E.

If the secondary FortiGate-7000E experiences an FIM failure, its status in the cluster does not change. However, in future negotiations the FortiGate-7000E with an FIM failure is less likely to become the primary FortiGate-7000E.

Link failure

If your HA configuration includes HA interface monitoring, if a primary FortiGate-7000E interface fails or is disconnected while a cluster is operating, a link failure occurs. When a link failure occurs, the FortiGate-7000Es in the cluster negotiate to select a new primary FortiGate-7000E. The link failure means that a that primary FortiGate-7000E with the most link failures will become the secondary and the FortiGate-7000E with the fewest link failures becomes the primary FortiGate-7000E.

Just as for a device failover, the new primary FortiGate-7000E sends gratuitous arp packets out all of its connected interfaces to inform attached switches to send traffic to it. Sessions then resume with the new primary FortiGate-7000E.

If the secondary FortiGate-7000E experiences a link failure, its status in the cluster does not change. However, in future negotiations a FortiGate-7000E with a link failure is less likely to become the primary FortiGate-7000E.

If one of the FortiGate-7000Es experiences an FIM or FPM failure and the other experiences a link failure, the FortiGate-7000E with the most operating FIMs or FPMs becomes the primary FortiGate-7000E, even if it is also experiencing a link failure.

FPM failure

If one or more FPMs in the primary FortiGate-7000E fails, the cluster renegotiates and the FortiGate-7000E with the most operating FPMs becomes the primary FortiGate-7000E. An FPM failure can occur if the FPM shuts down due to a software crash or hardware problem, or if the FPM is manually shut down or even removed from the chassis.

After the primary FortiGate-7000E experiences an FIM failure, the FortiGate-7000E with the most operating FPMs becomes the new primary FortiGate-7000E. The new primary FortiGate-7000E sends gratuitous arp packets out all of its connected interfaces to inform attached switches to send traffic to it. Sessions then resume with the new primary FortiGate-7000E.

If the secondary FortiGate-7000E experiences an FPM failure, its status in the cluster does not change. However, in future negotiations the FortiGate-7000E with an FPM failure is less likely to become the primary FortiGate-7000E.

Session failover

FortiGate-7000E session synchronization involves the primary FortiGate-7000E informing the secondary FortiGate-7000E of changes to the primary FortiGate-7000E connection and state tables, keeping the secondary FortiGate-7000E up-to-date with the traffic currently being processed by the cluster.

Session synchronization traffic uses the M1 and M2 interfaces. FortiGate-7000E does not support using the `session-sync-dev` option to use data interfaces for session synchronization. The M1 and M2 interfaces provide enough bandwidth for both HA heartbeat and session synchronization traffic, so additional session synchronization devices are not required. As well, keeping session synchronization traffic on the M1 and M2 interfaces separates session synchronization traffic from data traffic.

After an HA failover, because of session synchronization the new primary FortiGate-7000E recognizes open sessions that were being handled by the cluster. The sessions continue to be processed by the new primary FortiGate-7000E and are handled according to their last known state.

Primary FortiGate-7000E recovery

If a primary FortiGate-7000E recovers after a device, FIM, link, or FPM failure, it will operate as the secondary FortiGate-7000E. If `override` is enabled; however, when the FortiGate-7000E recovers, the cluster will renegotiate and the FortiGate-7000E with the highest device priority becomes the primary FortiGate-7000E.

Setting up HA management connections

Fortinet recommends the following configurations for redundant management connections to a FortiGate-7000E 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-7000E configuration to set up redundant management connections. However, specific switch configurations are required for each of these configurations as described below.

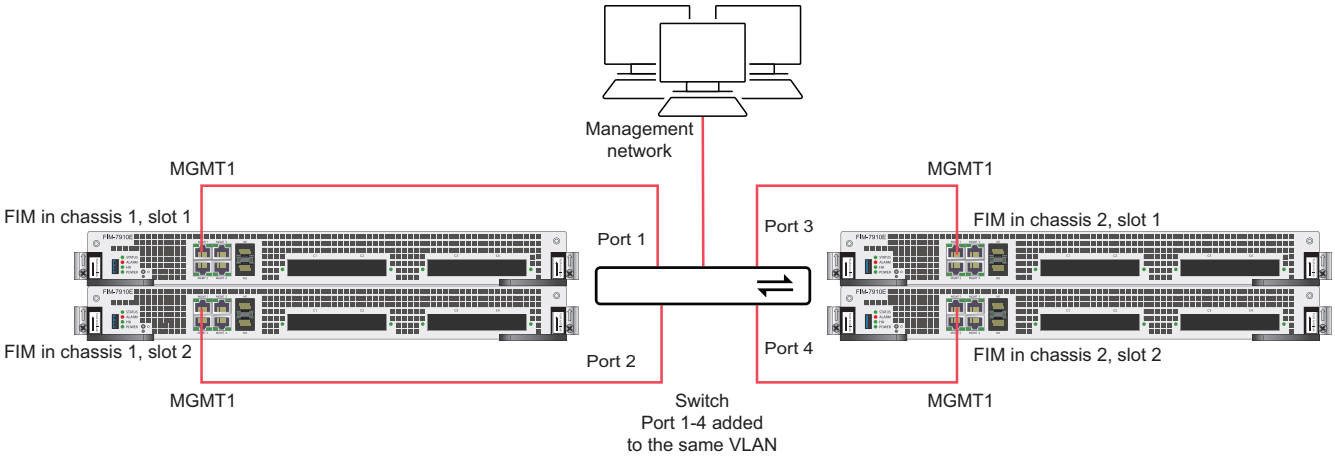
LACP is not supported for the mgmt aggregate interface.

Setting up single management connections to each of the FIMs

The simplest way to provide redundant management connections to a FortiGate-7000E 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-7000E HA redundant management connections



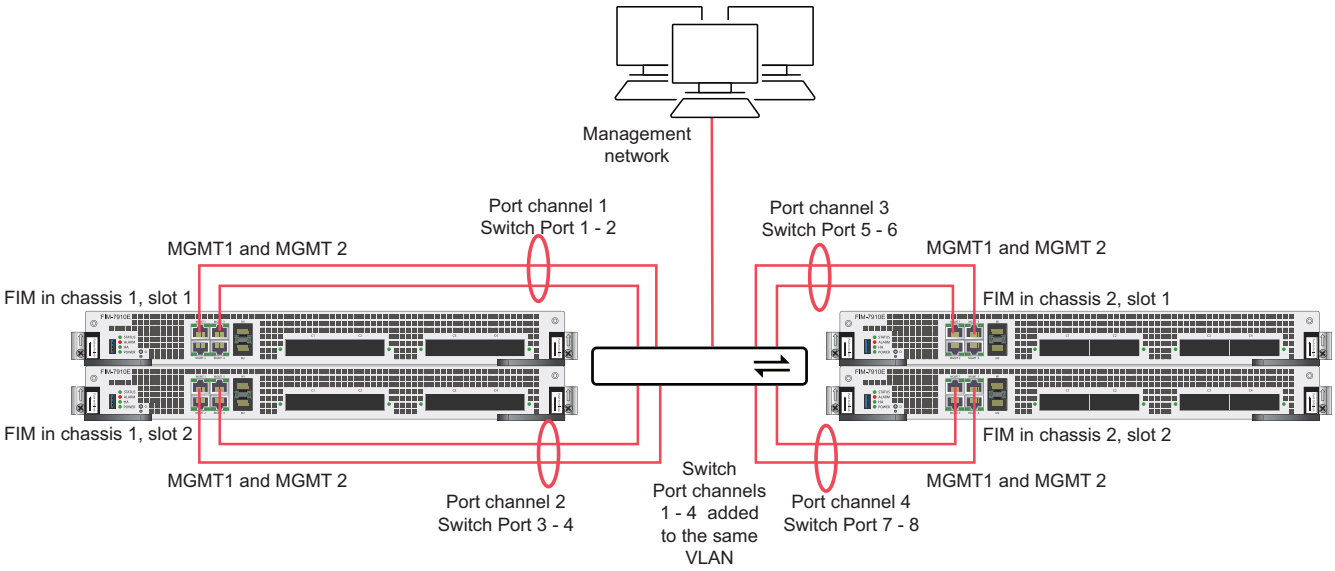
Setting up redundant management connections to each of the FIMs

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-7000E HA redundant management connections with redundant connections to each FIM



HA reserved management interfaces

You can edit an HA cluster and add one or more VLAN interfaces to the FortiGate-7000E management interface LAG and configure these VLAN interfaces to be HA reserved management interfaces. You can then log into each FortiGate-7000E in the cluster and configure its reserved management interfaces with IP addresses and other custom interface settings as required. You can also configure routing for each reserved management interface. The result is that each FortiGate-7000E in the cluster has its own management interface or interfaces and each of these interfaces has its own IP address that is not synchronized to the other FortiGate-7000E in the cluster.

After adding one or more VLAN interfaces to the FortiGate-7000E management interface LAG, to configure an HA reserved management interface from the GUI, go to **System > HA** and enable **Management Interface Reservation**. Select one or more interfaces to be HA reserved management interfaces. Optionally configure routing for each reserved management interface. This routing configuration is not synchronized and can be configured separately for each FortiGate-7000E in the cluster.

To configure an HA reserved management interface from the CLI:

```
config system ha
   set mode a-p
   set ha-mgmt-status enable
   set ha-direct enable
      config ha-mgmt-interfaces
         edit 0
```

```
            set interface <interface>
            set dst <destination-ip>
            set gateway <gateway-ip>
            set gateway6 <gateway-ipv6-ip>
        end
    end
```

Enabling `ha-direct` from the CLI is required if you plan to use the HA reserved management interface for SNMP, remote logging, or communicating with FortiSandbox. Enabling `ha-direct` is also required for some types of remote authentication, but is not required for RADIUS remote authentication.

`<interface>` can be any VLAN interface that you have added to the FortiGate-7000E management interface (mgmt).

For more information, see Out-of-band management.

HA in-band management for management interfaces

The FortiGate-7000E now supports FGCP HA in-band management for FortiGate-7000E management interfaces and the management interface LAG.

HA in-band management allows you to add a second management IP address to one or more FortiGate-7000E management interfaces. The management IP address is accessible from the network that the interface is connected to. This setting is not synchronized, so each FortiGate-7000E in the cluster can have their own in-band management IP addresses; providing management access to the secondary FortiGate-7000E.

FortiGate-7000E does not support HA in-band management for data interfaces.

HA in-band management configuration:

```
config vdom
   edit mgmt-vdom
      config system interface
         edit mgmt
            set management-ip <ip address>
         end
```

You can also remove individual mgmt interfaces from the FortiGate-7000E management interface LAG and add an in-band management address to these interfaces.

The `management-ip` option is available only when HA is enabled.

To support HA in-band management, the FortiGate-7000E handles Cluster virtual MAC addresses in the same way as other FortiGates.

Virtual clustering

FortiGate-7000E supports virtual clustering with two FortiGate-7000Es operating in Multi VDOM mode. Virtual clustering is not supported for Split-Task VDOM mode.

A virtual cluster consists of two FortiGate-7000Es operating in active-passive HA mode with Multi VDOM mode enabled. Virtual clustering is an extension of FGCP HA that uses VDOM partitioning to send traffic for some VDOMs to the primary FortiGate-7000E and traffic for other VDOMs to the secondary FortiGate-7000E. Distributing traffic between the FortiGate-7000Es in a virtual cluster is similar to load balancing and can potentially improve overall throughput. You can adjust VDOM partitioning at any time to optimize traffic distribution without interrupting traffic flow.

VDOM partitioning distributes VDOMs between two virtual clusters (virtual cluster 1 and virtual cluster 2). When configuring virtual clustering you would normally set the device priority of virtual cluster 1 higher for the primary FortiGate-7000E and the device priority of virtual cluster 2 higher for the secondary FortiGate-7000E. With this configuration, all traffic in the VDOMs in virtual cluster 1 is processed by the primary FortiGate-7000E and all traffic in the VDOMs in virtual cluster 2 is processed by the secondary FortiGate-7000E. The FGCP selects the primary and secondary FortiGate-7000E whenever the cluster negotiates. The primary FortiGate-7000E can dynamically change based on FGCP HA primary unit selection criteria.

If a failure occurs and only one FortiGate-7000E continues to operate, all traffic fails over to that FortiGate-7000E, similar to normal FGCP HA. When the failed FortiGate-7000Erejoins the cluster, the configured traffic distribution is restored.

For more information about virtual clustering see HA virtual cluster setup.

If you don't want active-passive virtual clustering to distribute traffic between FortiGate-7000Es, you can configure VDOM partitioning to send traffic for all VDOMs to the primary FortiGate-7000E. The result is the same as standard active-passive FCGP HA, all traffic is processed by the primary FortiGate-7000E.

Virtual clustering creates a cluster between instances of each VDOM on the two FortiGate-7000Es in the virtual cluster. All traffic to and from a given VDOM is sent to one of the FortiGate-7000Es where it stays within its VDOM and is only processed by that VDOM. One FortiGate-7000E is the primary FortiGate-7000E for each VDOM and one FortiGate-7000E is the secondary FortiGate-7000E for each VDOM. The primary FortiGate-7000E processes all traffic for its VDOMs. The secondary FortiGate-7000E processes all traffic for its VDOMs.

The HA heartbeat and session synchronization provides the same HA services in a virtual clustering configuration as in a standard HA configuration. One set of HA heartbeat interfaces provides HA heartbeat and session synchronization services for all of the VDOMs in the cluster. You do not have to add a heartbeat interface for each VDOM.

Limitations of FortiGate-7000E virtual clustering

FortiGate-7000E virtual clustering includes the following limitations:

- Virtual clustering supports two FortiGate-7000Es only.
- Active-passive HA mode is supported, active-active HA is not.
- The root and mgmt-vdom VDOMs must be in virtual cluster 1 (also called the primary virtual cluster).
- A VLAN must be in the same virtual cluster as the physical interface or LAG that the VLAN has been added to. The VLAN can be in the same VDOM as its physical interface or LAG or in a different VDOM, as long as both VDOMs are in the same virtual cluster.
- The interfaces that are created when you add an inter-VDOM link must be in the same virtual cluster as the inter-VDOM link. You can change the virtual cluster that an inter-VDOM link is in by editing the inter-VDOM link and changing the `vcluster` setting.

Virtual clustering VLAN/VDOM limitation

In a FortiGate-7000E virtual clustering configuration, a VLAN must be in the same virtual cluster as the physical interface, LAG, or redundant interface that the VLAN has been added to. The VLAN can be in the same VDOM as its physical interface, LAG, or redundant interface or in a different VDOM, as long as both VDOMs are in the same virtual cluster.

If virtual clustering has already been set up, when adding VLANs, GUI and CLI error checking prevents you from adding a VLAN to a VDOM that is in a different virtual cluster than the physical interface, LAG, or redundant interface that you are attempting to add the VLAN to. However, error checking can't prevent this problem if you configure the VLANs before setting up virtual clustering or if you move VDOMs to different virtual clusters after adding the VLANs.

A recommended strategy for preventing this problem could involve the following steps:

1. Start by setting up virtual clustering before creating new VDOMs.
2. Create a placeholder VDOM and add it to virtual cluster 2.
3. Separate traffic interfaces between the root VDOM in virtual cluster 1 and the placeholder VDOM in virtual cluster 2.

   Based on network planning you can create an even distribution of planned traffic volume between the two virtual clusters.
4. Build up your configuration by adding more VDOMs, LAGs, redundant interfaces, and VLANs as required, making sure to keep VLANs in the same virtual cluster as their parent interfaces, LAGs, or redundant interfaces.

Example incorrect VLAN configuration

Consider the following FortiGate-7000E virtual clustering example, which shows how traffic can be blocked by this limitation:

- Three data traffic VDOMs: root, Engineering, and Marketing.
- One LAG interface: LAG1 in the root VDOM.
- Two VLAN interfaces added to LAG1: vlan11 and vlan12.
  - vlan11 is added to the Engineering VDOM.
  - vlan12 is added to the Marketing VDOM.
- The root and Engineering VDOMs are in virtual cluster 1.
- The Marketing VDOM is in virtual cluster 2.

As a result of this configuration:

- vlan11 is in the Engineering VDOM, which is in virtual cluster 1. vlan11 is also in LAG1, which is in the root VDOM, also in virtual cluster 1. vlan11 and its LAG are in the same virtual cluster. Traffic can pass through vlan11.
- vlan12 is in the Marketing VDOM, which is in virtual cluster 2. vlan12 is also in LAG1, which is in the root VDOM, in virtual cluster 1. vlan12 and its LAG are in different virtual clusters. Traffic cannot pass through vlan12.

Configuring virtual clustering

Configuring virtual clustering is the same as configuring standard FCGP HA with the addition of VDOM partitioning. Using VDOM partitioning, you can control the distribution of VDOMs, and the traffic they process, between the FortiGates in the cluster.

VDOM partitioning can be thought of in two parts. First, there is configuring the distribution of VDOMs between two virtual clusters. By default, all VDOMS are in virtual cluster 1, virtual cluster 1 is associated with the primary FortiGate-

7000E, and the primary FortiGate-7000E processes all traffic. If you want traffic to be processed by the secondary FortiGate-7000E, you need to enable virtual cluster 2, move some of the VDOMs to it, and associate virtual cluster 2 with the secondary FortiGate-7000E.

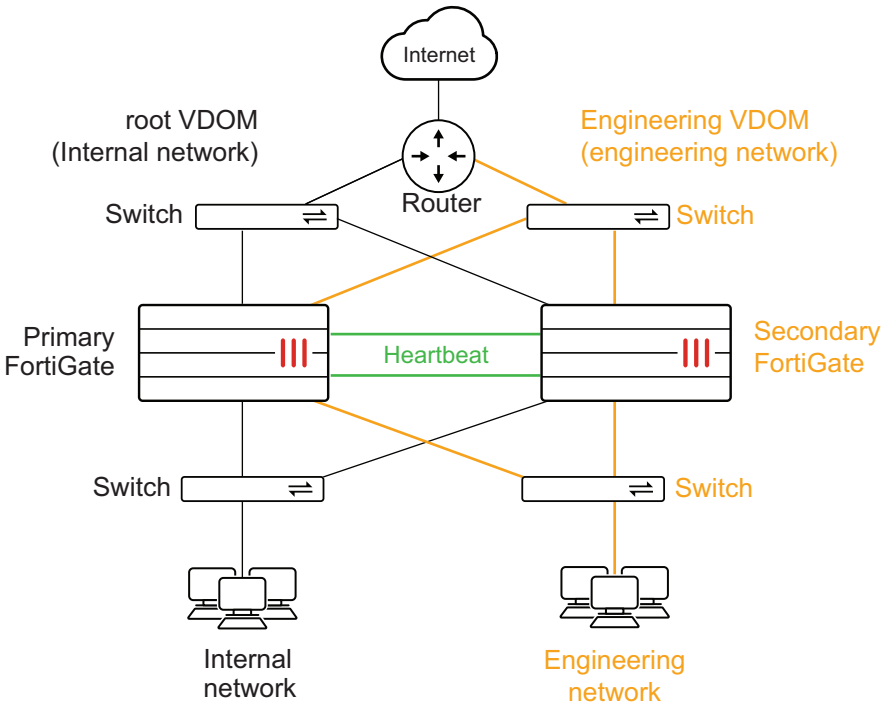
You associate a virtual cluster with a FortiGate-7000E using device priorities. The FortiGate-7000E with the highest device priority is associated with virtual cluster 1. To associate a FortiGate-7000E with virtual cluster 2, you must enable virtual cluster 2 and set virtual cluster 2 device priorities on each FortiGate-7000E. The FortiGate-7000E with the highest virtual cluster 2 device priority processes traffic for the VDOMs added to virtual cluster 2. (Reminder: device priorities are not synchronized.)

Normally, you would set the virtual cluster 1 device priority for the primary FortiGate-7000E and the virtual cluster 2 device priority higher for the secondary FortiGate-7000E. Then the primary FortiGate-7000E would process virtual cluster 1 traffic and the secondary FortiGate-7000E would process virtual cluster 2 traffic.

Enabling virtual cluster 2 also turns on HA override for virtual cluster 1 and 2. Enabling override is required for virtual clustering to function as configured. Enabling override causes the cluster to negotiate every time the cluster state changes. If override is not enabled, the cluster may not negotiate as often. While more frequent negotiation may cause more minor traffic disruptions, with virtual clustering its more important to negotiate after any state change to make sure the configured traffic flows are maintained.

The figure below shows a simple FortiGate-7000E virtual cluster that provides redundancy and failover for two networks. The configuration includes two VDOMs. The root VDOM handles internal network traffic and the Engineering VDOM handles Engineering network traffic. VDOM partitioning has been set up to send all root VDOM traffic to the primary FortiGate and all Engineering VDOM traffic to the secondary FortiGate.

Example virtual clustering configuration



Primary FortiGate-7000E configuration

The primary FortiGate-7000E configuration:

- Sets the primary FortiGate-7000E to be chassis 1.
- Enables virtual cluster 2 (`vcluster2`) to enable virtual clustering.
- Enables override for virtual cluster 1.
- Sets the virtual cluster 1 device priority to 200.
- Enables override for virtual cluster 2 (`secondary-vcluster`).
- Sets the virtual cluster 2 device priority to 50.
- Adds the Engineering VDOM to virtual cluster 2 (all VDOMs remain in virtual cluster 1 unless you add them to virtual cluster 2).

```
config system ha
   set group-id 6
   set group-name <name>
   set mode a-p
   set password <password>
   set hbdev 1-M1 50 2-M1 50 1-M2 50 2-M2 50
   set chassis-id 1
   set vcluster2 enable
   set override enable
   set priority 200
   config secondary-vcluster
      set override enable
      set priority 50
      set vdom Engineering
   end
```

Secondary FortiGate configuration

The secondary FortiGate configuration:

- Sets the secondary FortiGate to be chassis 2.
- Enables virtual cluster 2 (`vcluster2`) to enable virtual clustering.
- Enables override for virtual cluster 1.
- Sets the device priority of virtual cluster 1 to 50.
- Enables override for virtual cluster 2 (`secondary-vcluster`).
- Sets the virtual cluster 2 device priority to 200.
- You do not need the add the Engineering VDOM to virtual cluster 2, the configuration of the VDOMs in virtual cluster 2 is synchronized from the primary FortiGate.

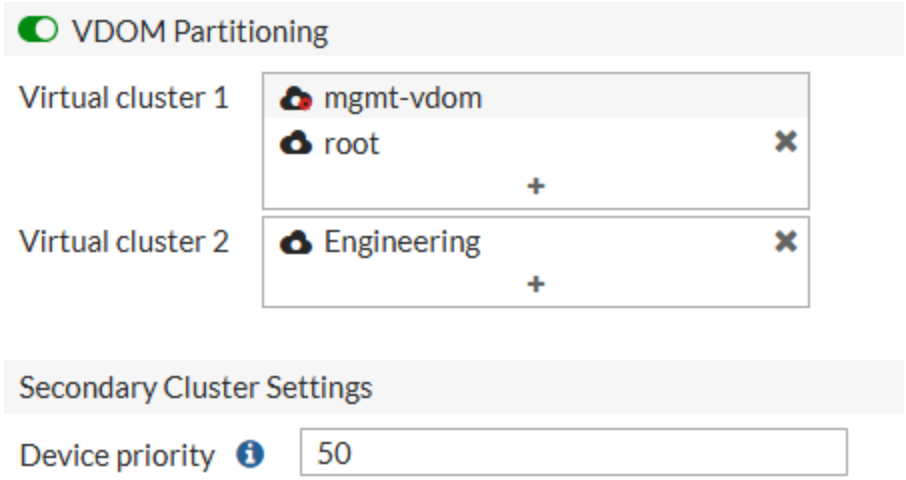
```
config system ha
   set group-id 6
   set group-name <name>
   set mode a-p
   set password <password>
   set bdev "1-M1" 50 "2-M1" 50 "1-M2" 50 "2-M2" 50
   set chassis-id 2
   set vcluster2 enable
   set override enable
   set priority 50
   config secondary-vcluster
      set override enable
      set priority 200
      set vdom Engineering
   end
```

Since the primary FortiGate-7000E has the highest device priority, it processes all traffic for the VDOMs in virtual cluster 1. Since the secondary FortiGate-7000E has the highest virtual cluster 2 device priority, it processes all traffic for the VDOM in virtual cluster 2. The primary FortiGate-7000E configuration adds the VDOMs to virtual cluster 2. All you have to configure on the secondary FortiGate-7000E for virtual cluster 2 is the virtual cluster 2 (or secondary-vcluster) device priority.

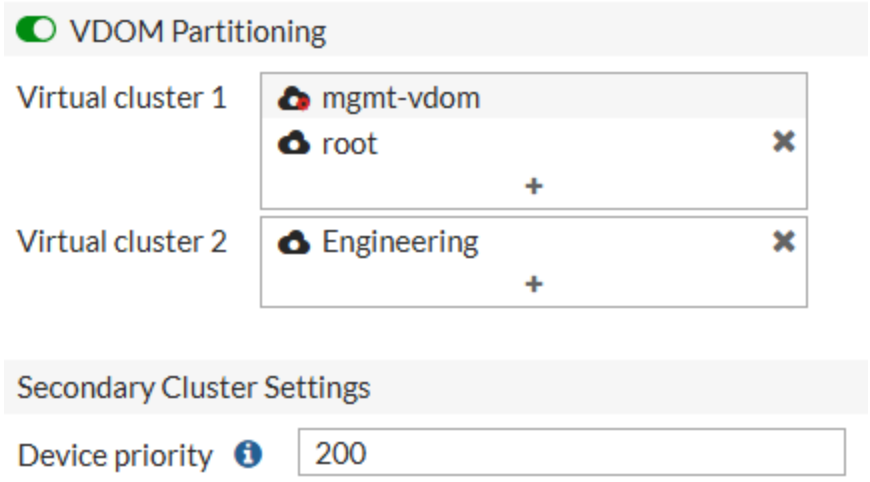
Virtual cluster GUI configuration

From the GUI, you configure virtual clustering from the **Global** menu by going to **System > HA**, configuring HA settings and VDOM Partitioning.

Primary FortiGate VDOM partitioning



Secondary FortiGate VDOM partitioning



HA cluster firmware upgrades

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

If `uninterruptible-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 uninterruptible-upgrade enable
   set session-pickup enable
end
```

When these settings are enabled, the primary FortiGate-7000E primary FIM uploads firmware to the secondary FortiGate-7000E primary FIM, which uploads the firmware to all of the modules in the secondary FortiGate-7000E. Then the modules in the secondary FortiGate-7000E upgrade their firmware, reboot, and resynchronize.

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

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

As well some firmware upgrades may not support `uninterruptible-upgrade`. For example, `uninterruptible-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 `uninterruptible-upgrade` is supported to upgrade to that version.

To make sure a FortiGate-7000E firmware upgrade is successful, before starting the upgrade Fortinet recommends you use health checking to make sure the FIMs and FPMs are all synchronized and operating as expected.

If you are following a multi-step upgrade path, you should re-do health checking after each upgrade step to make sure all components are synchronized before the next step.

You should also perform a final round of health checking after the firmware upgrade process is complete.

For recommended health checking commands, see the following Fortinet community article:

Technical Tip: FortiGate-6000/7000 Chassis health check commands.

Distributed clustering

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

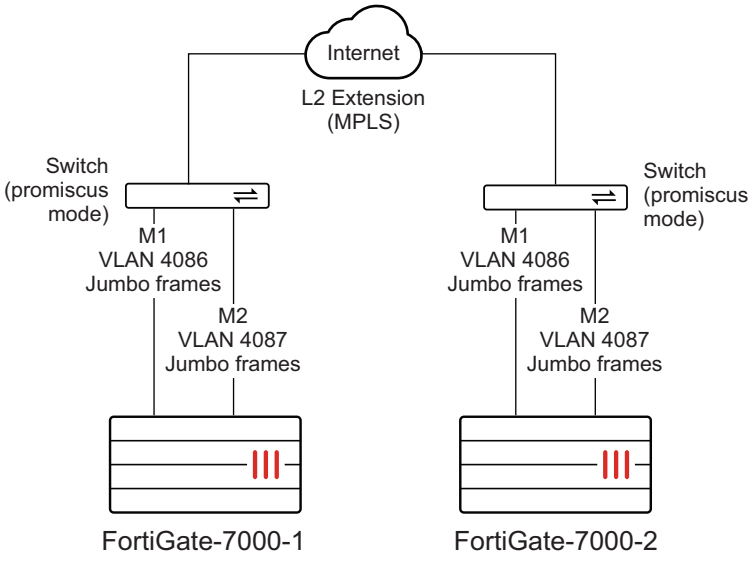
Just like any FortiGate-7000E HA configuration, distributed FortiGate-7000E HA requires heartbeat communication between the FortiGate-7000Es over the M1 and M2 interfaces. In a distributed FortiGate-7000E HA configuration this heartbeat communication can take place over the Internet or over other transmission 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-7000E 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-7000Es. 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 93.

Modifying heartbeat timing

If the FortiGate-7000Es in the HA cluster do not receive heartbeat packets on time, the FortiGate-7000Es in the HA configuration may each determine that the other FortiGate-7000E 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-7000Es become too busy to handle the heartbeat traffic. Also, in a distributed clustering configuration the round trip time (RTT) between the FortiGate-7000Es may be longer the expected time between heartbeat packets.

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

Even with these delays, the FortiGate-7000E 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-7000E does not receive 6 heartbeat packets it determines that the other FortiGate-7000E in the cluster has failed. The range is 1 to 60 packets.

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

Setting a FortiGate-7000E to always be the primary FortiGate-7000E

You can use the following command from the CLI of a FortiGate-7000E in an HA configuration to cause the FortiGate-7000E that you are logged into to always operate as the primary FortiGate-7000E, effectively blocking HA failovers.

```
diagnose sys ha set-as-primary enable
```

If the FortiGate-7000E that you are logged into is already the primary, the cluster continues to operate normally. If you are logged into the backup FortiGate-7000E, a failover occurs and this FortiGate-7000E becomes the primary FortiGate-7000E.

Command syntax:

```
diagnose sys ha set-as-primary {disable | enable | status}
```

`disable` the default, HA failovers can occur.

`enable` the FortiGate-7000E that you are logged into becomes and remains the primary FortiGate in the HA cluster.

`status` view the `set-as-primary` status of the FortiGate-7000E that you have logged into.

This command is intended to be used during troubleshooting and not for normal operation. Because this is a diagnose command, the command is reset to `disable` when the FortiGate restarts.

After you have finished troubleshooting you can either restart the cluster to restore normal operation or enter the following command:

```
diagnose sys ha set-as-primary disable
```

This may cause an HA failover depending on your HA configuration. For example, if override is enabled the cluster may renegotiate to select a primary FortiGate-7000E.

Changing how long routes stay in a cluster unit routing table

You can use the HA route time to live (`route-ttl`) option to control how long routes remain active in the new primary FortiGate-7000E after an FGCP HA failover. The default `route-ttl` is 600 seconds. The range is 5 to 3600 seconds (one hour). You can use the following command to change the `route-ttl` time.

```
config system ha
   set route-ttl <time>
end
```

FortiOS 6.0.6 for FortiGate-7000E does not support the `route-wait` and `route-hold` options.

To maintain communication sessions through a new primary FortiGate-7000E, routes remain active in the routing table for the `route-ttl` time while the new primary FortiGate-7000E acquires new routes. Normally keeping `route-ttl` to the default value of 600 seconds (10 minutes) is acceptable because acquiring new routes and populating the routing tables of multiple FIMs and FPMs can take a few minutes.

If the primary FortiGate-7000E needs to acquire a very large number of routes, or if for other reasons there is a delay in acquiring all routes, the primary FortiGate-7000E may not be able to maintain all communication sessions after a failover.

You can increase the `route-ttl` time if you find that communication sessions are lost after a failover. Increasing the `route-ttl` time allows the primary unit to use synchronized routes that are already in the routing table for a longer period of time while waiting to acquire new routes.

For more information, see Synchronizing kernel routing tables.

Session failover (session-pickup)

Session failover means that after a failover, communications sessions resume on the new primary FortiGate-7000E 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-7000E HA. If sessions pickup is enabled, while the FortiGate-7000E HA cluster is operating the primary FortiGate-7000E informs the secondary FortiGate-7000E of changes to the primary FortiGate-7000E connection and state tables for TCP and UDP sessions passing through the cluster, keeping the secondary FortiGate-7000E up-to-date with the traffic currently being processed by the cluster.

After a failover the new primary FortiGate-7000E recognizes open sessions that were being handled by the cluster. The sessions continue to be processed by the new primary FortiGate-7000E 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-7000E TCP and connectionless session tables are synchronized to the secondary FortiGate-7000E. As soon as a new session is added to the primary FortiGate-7000E session table, that session is synchronized to the secondary FortiGate-7000E. This synchronization happens as quickly as possible to keep the session tables synchronized.

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

FortiGate-7000E FGSP

FortiGate-7000E supports the FortiGate Session Life Support Protocol (FGSP) (also called standalone session sync) to synchronize sessions among up to four FortiGate-7000Es. FortiGate-7000E also supports FGSP between FGCP clusters.

For details about FGSP, see: FGSP.

You have the following options for selecting interfaces to use for FGSP session synchronization:

- Up to eight physical data interfaces.
- One or more data interface LAGs.
- VLANs added to the data interfaces or data interface LAGs.
- The M1 or M2 interface of either FIM.
- A LAG consisting of the M1 and M2 interfaces of one or both FIMs.

You can use configuration synchronization to synchronize the configurations of the FortiGate-7000Es in the FGSP deployment (see Standalone configuration synchronization on page 107). You can use the M1 and M2 interfaces for

configuration synchronization. You can also configure the FortiGate-7000Es separately or use FortiManager to keep key parts of the configuration, such as security policies, synchronized.

FortiGate-7000E FGSP support has the following limitations:

- FortiGate-7000E FGSP doesn't support setting up IPv6 session filters using the `config session-sync-filter` option.
- Asymmetric IPv6 SCTP traffic sessions are not supported. These sessions are dropped.
- Inter-cluster session synchronization, or FGSP between FGCP clusters, is not supported for the FortiGate-7000E.
- FGSP IPsec tunnel synchronization is not supported.
- Fragmented packet synchronization is not supported.

FortiGate-7000E FortiOS Carrier GTP with FGSP support

FortiGate-7000E FGSP clusters licensed for FortiOS Carrier support synchronizing GTP tunnels among up to four FortiGate-7000E chassis. No special configuration is required to support this feature. Just a standard FGSP configuration and standard GTP profiles and policies.

FGSP session synchronization options

FortiGate-7000E 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 the FGSP. FGCP 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 FortiGate-7000Es).

Enabling session synchronization

Use the following command to synchronize TCP and SCTP sessions between FortiGate-7000Es.

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

Enabling `session-pickup` also enables 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 deployment.

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.

Synchronizing sessions older than 30 seconds

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

Using data interfaces for FGSP session synchronization

FortiGate-7000E FGSP supports using up to eight physical data interfaces for FGSP session synchronization.

Use the following command to select up to eight physical data interfaces to use for FGSP session synchronization:

```
config system standalone-cluster
   set data-intf-session-sync-dev <interface-name> [<interface-name> ...]
end
```

You can use these individual interfaces or VLANs added to these interfaces for FGSP session synchronization. You can also create LAGs of two or more of these physical interfaces and use the LAGs for FGSP session synchronization. You can also add a VLAN to a LAG and use this VLAN for FGSP session synchronization.

Fortinet recommends:

- Use a data interface LAG for FGSP session synchronization. A LAG supports higher throughput than a single interface and also provides redundancy.
- To improve redundancy, the data interface LAG should include interfaces from both FIMs.
- Do not use FGSP session synchronization data interfaces for other traffic.
- Enable jumbo frames on the data interfaces, LAGs, and VLANs that you use for FGSP session synchronization.

- Keep the FGSP session synchronization data interfaces in a separate dedicated VDOM. Any VLANs you add to these interfaces or LAGs that you create for FGSP session synchronization should also be in the same dedicated VDOM. You must then specify this VDOM as the `peervd` in the `config system cluster-sync` configuration.

  For example, you could create a VDOM called `fgsp-sync` and add the data interfaces, VLANs and LAGs that you are using for FGSP session synchronization to that VDOM. Then you can create the following `config system cluster-sync` instance to synchronize sessions from the root VDOM:

```
config system cluster-sync
   edit 1
      set peervd fgsp-sync
      set peerip <ip-address>
      set syncvd root
   end
```

Synchronizing sessions between FortiGate-7000E FGCP clusters

FortiGate-7000E supports using FGSP to synchronize sessions among up to four FortiGate-7000E FGCP clusters. All of the FortiGate-7000Es must be the same hardware model.

FGSP between FGCP clusters synchronizes sessions between the primary FortiGate-7000Es in each cluster. FGCP HA then handles session synchronization between FortiGate-7000Es in each FGCP cluster.

For details about FGSP between FGCP clusters, see: Synchronizing sessions between FGCP clusters.

You can use data interfaces or data interface LAGs as FGSP session synchronization interfaces. The M1 and M2 interfaces are used for FGCP HA heartbeat between the FortiGate-7000Es in each FGCP cluster.

FortiGate-7000E synchronizing sessions between FGCP clusters has the following limitations:

- The FGCP clusters cannot be configured for virtual clustering.
- NAT between the session synchronization interfaces is not supported.
- Standalone configuration synchronization between the FCGP clusters is not supported.
- Inter-cluster session synchronization doesn't support setting up IPv6 session filters using the `config session-sync-filter` option.
- When ICMP load balancing is set to `to-master`, ICMP packets are not installed on the DP processor. In an FGSP between FGCP session synchronization configuration with an asymmetry topology, synchronized ICMP packets will be dropped if the clusters have selected a different primary FPM. To avoid this possible traffic loss, set `dp-icmp-distribution-method` to `src-ip`, `dst-ip`, or `src-dst-ip`.
- Asymmetric IPv6 SCTP traffic sessions are not supported. These sessions are dropped.
- FGSP IPsec tunnel synchronization is not supported.
- Session synchronization packets cannot be fragmented. So the MTU for the session synchronization interface should be supported by the network.
- To reduce the number of failovers and the amount of session synchronization traffic, configuring HA override on the FGCP clusters is not recommended.

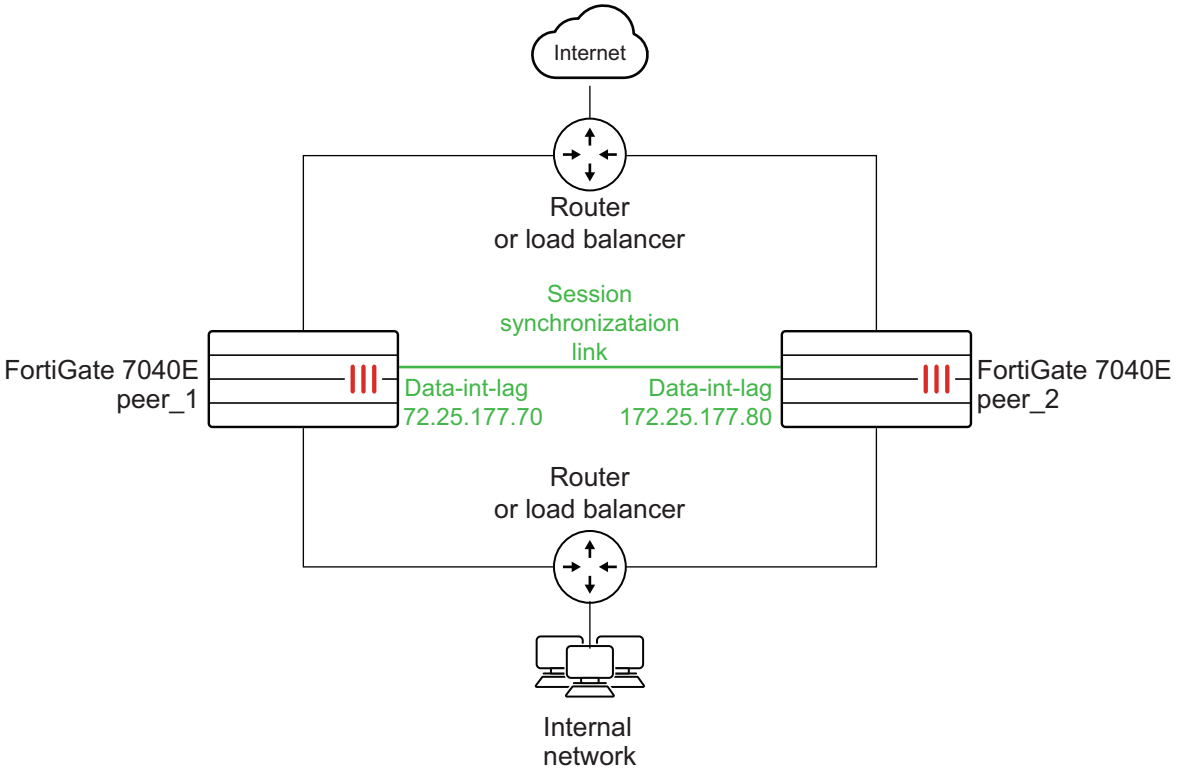
Example FortiGate-7000E FGSP session synchronization with a data interface LAG

This example shows how to configure FGSP to synchronize sessions between two FortiGate-7040Es for the root VDOM and for a second VDOM, named vdom-1. For FGSP session synchronization, the example uses a data interface LAG that includes the 1-A13, 1-A14, 1-A15, 1-A16, 2-A13, 2-A14, 2-A15, and 2-A16 interfaces.

To set up the configuration, start by giving each FortiGate-7040E a different host name to make them easier to identify. This example uses peer_1 and peer_2. On each FortiGate-7040E, create a VDOM named fgsp-sync and move the 1-A13, 1-A14, 1-A15, 1-A16, 2-A13, 2-A14, 2-A15, and 2-A16 interfaces to this VDOM. Then create a LAG named Data-int-lag, also in the fgsp-sync VDOM, that includes the 1-A13, 1-A14, 1-A15, 1-A16, 2-A13, 2-A14, 2-A15, and 2-A16 interfaces. The LAGs on both FortiGate-7040Es are on the 172.25.177.0/24 network.

This example also adds standalone configuration synchronization using the 1-M1 and 1-M2 interfaces and sets the peer_1 device priority higher so that it becomes the config sync primary. Once configuration synchronization is enabled, you can log into peer_1 and add firewall policies and make other configuration changes and these configuration changes will be synchronized to peer_2. For information about configuration synchronization, including its limitations, see Standalone configuration synchronization on page 107.

Example FortiGate-7000 FGSP configuration using data interface LAGs



1. Configure the routers or load balancers to distribute sessions to the two FortiGate-7040Es.
2. Change the host names of the FortiGate-7040Es to peer_1 and peer_2.
3. Configure network settings for each FortiGate-7040E to allow them to connect to their networks and route traffic.
4. Add the vdom-1 and fgsp-sync VDOMs to each FortiGate-7040E.
5. Also on each FortiGate-7040E, move the 1-A13, 1-A14, 1-A15, 1-A16, 2-A13, 2-A14, 2-A15, and 2-A16 interfaces to the fgsp-sync VDOM.
6. On peer_1, configure the 1-A13, 1-A14, 1-A15, 1-A16, 2-A13, 2-A14, 2-A15, and 2-A16 interfaces to be FGSP session synchronization data interfaces.

```
config system standalone-cluster
   set standalone-group-id 6
   set group-member-id 1
   set data-intf-session-sync-dev 1-A13 1-A14 1-A15 1-A16 2-A13 2-A14 2-A15 2-A16
end
```

7. On peer_1, add a data interface LAG to the fgsp-sync VDOM.

```
config system interface
   edit Data-int-lag
      set type aggregate
      set vdom fgsp-sync
      set member 1-A13 1-A14 1-A15 1-A16 2-A13 2-A14 2-A15 2-A16
      set ip 172.25.177.70/24
      set mtu-override enable
      set mtu 9216
   end
```

   This configuration adds the data interface LAG to the fgsp-sync VDOM, includes the eight data interfaces configured to be FGSP session synchronization interfaces, and configures the LAG to support jumbo frames.

8. On peer_1, configure session synchronization for the root and vdom-1 VDOMs.

```
config system cluster-sync
   edit 1
      set peervd fgsp-sync
      set peerip 172.25.177.80
      set syncvd root vdom-1
   end
```

   `peervd` is `fgsp-sync` because the FGSP session synchronization data interfaces are in the fgsp-sync VDOM.

   `peerip` is the IP address of the data interface LAG added to peer_2.

   This configuration creates one `cluster-sync` instance that includes both VDOMs. You could have created a separate `cluster-sync` instance for each VDOM. If possible, however, avoid creating more than three `cluster-sync` instances. A fourth `cluster-sync` instance may experience reduced session synchronization performance.

9. On peer_1, enable configuration synchronization, enable session pickup, configure the heartbeat interfaces, and set a higher device priority. This makes peer_1 become the config sync primary.

```
config system ha
   set standalone-config-sync enable
   set session-pickup enable
   set session-pickup-connectionless enable
   set session-pickup-expectation enable
   set session-pickup-nat enable
   set priority 250
   set hbdev 1-M1 50 1-M2 50
end
```

10. On peer_2, configure the 1-A13, 1-A14, 1-A15, 1-A16, 2-A13, 2-A14, 2-A15, and 2-A16 interfaces to be FGSP session synchronization data interfaces.

```
config system standalone-cluster
   set standalone-group-id 6
   set group-member-id 2
   set data-intf-session-sync-dev 1-A13 1-A14 1-A15 1-A16 2-A13 2-A14 2-A15 2-A16
end
```

11. On peer_2, add a data interface LAG to the fgsp-sync VDOM:

```
config system interface
   edit Data-int-lag
      set type aggregate
      set vdom fgsp-sync
      set member 1-A13 1-A14 1-A15 1-A16 2-A13 2-A14 2-A15 2-A16
      set ip 172.25.177.80/24
      set mtu-override enable
      set mtu 9216
   end
```

This configuration adds the data interface LAG to the fgsp-sync VDOM, includes the eight data interfaces configured to be FGSP session synchronization interfaces, and configures the LAG to support jumbo frames.

12. On peer_2, configure session synchronization for the root and vdom-1 VDOMs.

```
config system cluster-sync
   edit 1
      set peervd fgsp-sync
      set peerip 172.25.177.70
      set syncvd root vdom-1
   end
```

13. On peer_2, enable configuration synchronization, enable session pickup, configure the heartbeat interfaces, and leave the device priority set to the default value.

```
config system ha
   set standalone-config-sync enable
   set session-pickup enable
   set session-pickup-connectionless enable
   set session-pickup-expectation enable
   set session-pickup-nat enable
   set hbdev 1-M1 50 1-M2 50
end
```

As sessions are forwarded by the routers or load balancers to one of the FortiGate-7040Es, the FGSP synchronizes the sessions to the other FortiGate-7040E. You can log into peer_1 and make configuration changes, which are synchronized to peer_2.

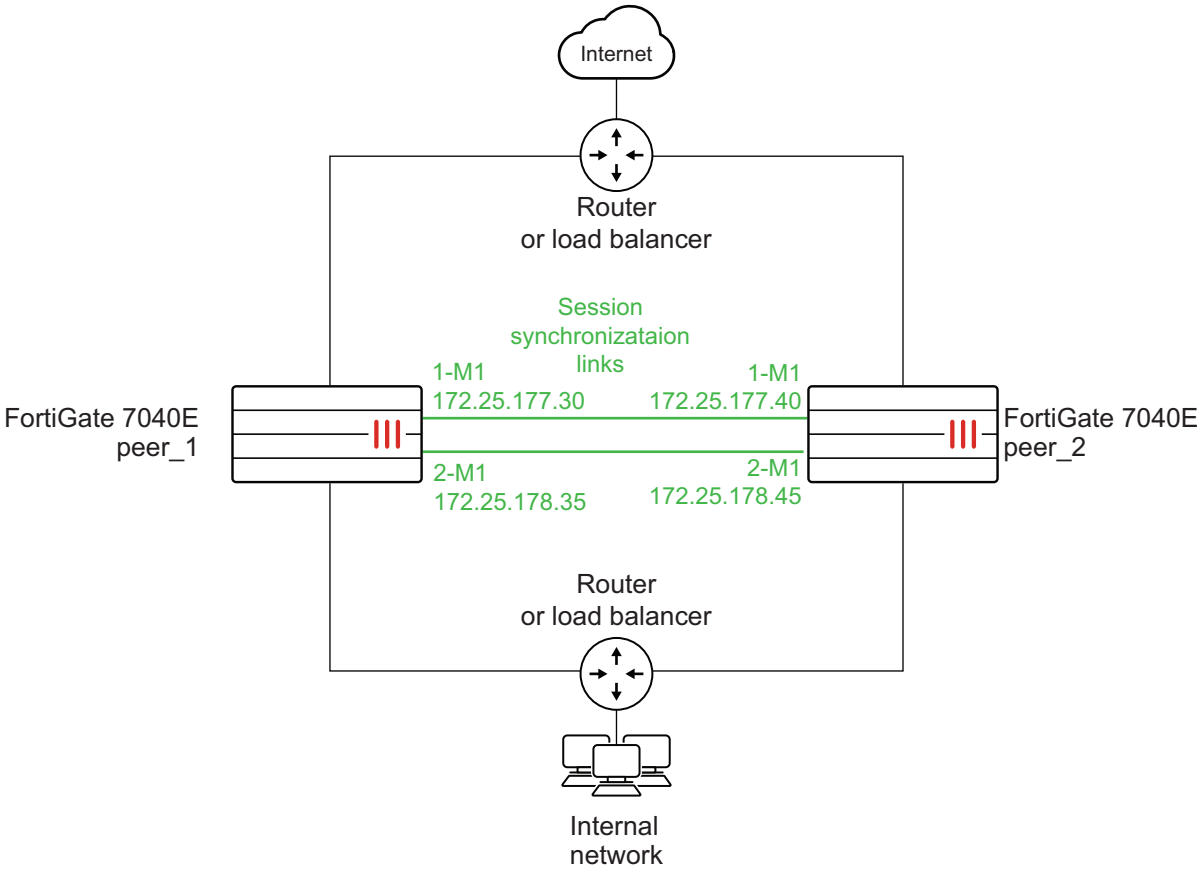
Example FortiGate-7000E FGSP configuration using 1-M1 interfaces

This example shows how to configure FGSP to synchronize sessions between two FortiGate-7040Es for the root VDOM and for a second VDOM, named vdom-1. The example uses the 1-M1 interface for root session synchronization and the 1-M2 interface for vdom-1 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.

The interfaces of the two FortiGate-7040Es must have their own IP addresses and their own networking configuration. You can give the FortiGate-7040Es different host names, in this example, peer_1 and peer_2, to make them easier to identify.

This example also adds configuration synchronization and sets the peer_1 device priority higher so that it becomes the config sync primary. Once configuration synchronization is enabled, you can log into peer_1 and add firewall policies and make other configuration changes and these configuration changes will be synchronized to peer_2. For information about configuration synchronization, including its limitations, see Standalone configuration synchronization on page 107.

Example FortiGate 7000E FGSP configuration



1. Configure the routers or load balancers to distribute sessions to the two FortiGate-7040s.
2. Change the host names of the FortiGate-7040Es to peer_1 and peer_2.
3. Configure network settings for each FortiGate-7040E to allow them to connect to their networks and route traffic.
4. Add the vdom-1 VDOM to each FortiGate-7040E.
5. On peer_1, set up the standalone-cluster configuration to use 1-M1 and 1-M2 as the FGSP session synchronization interfaces.

```
config system standalone-cluster
   set standalone-group-id 4
   set group-member-id 1
   set session-sync-dev 1-M1 1-M2
end
```

6. On peer_1 configure the 1-M1 and 1-M2 interfaces 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
```

7. On peer_1, configure session synchronization for the root and vdom-1 VDOMs.

```
config system cluster-sync
```

```
   edit 1
      set peervd mgmt-vdom
      set peerip 172.25.177.40
      set syncvd root
   next
   edit 2
      set peervd mgmt-vdom
      set peerip 172.25.178.45
      set syncvd vdom-1
   next
```

For the root vdom, `peervd` will always be `mgmt-vdom` and `peerip` is the IP address of the 1-M1 interface of peer_2.

For vdom-1, `peervd` will always be `mgmt-vdom` and `peerip` is the IP address of the 1-M2 interface of peer_2.

8. On peer_1, enable configuration synchronization, enable session pickup, configure the heartbeat interfaces, and set a higher device priority. This makes peer_1 become the config sync primary.

```
config system ha
   set standalone-config-sync enable
   set session-pickup enable
   set session-pickup-connectionless enable
   set session-pickup-expectation enable
   set session-pickup-nat enable
   set priority 250
   set hbdev 1-M1 50 1-M2 50
end
```

9. On peer_2, set up the standalone-cluster configuration to use 1-M1 and 1-M2 as the FGSP session synchronization interfaces.

```
config system standalone-cluster
   set standalone-group-id 4
   set group-member-id 2
   set session-sync-dev 1-M1 1-M2
end
```

10. On peer_2 configure the 1-M1 and 1-M2 interfaces 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
```

11. On peer_2, configure session synchronization for the root and vdom-1 VDOMs.

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

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

For vdom-1, `peervd` will always be `mgmt-vdom` and `peerip` is the IP address of the 1-M2 interface of peer_1.

12. On peer_2, enable configuration synchronization, enable session pickup, configure the heartbeat interfaces, and leave the device priority set to the default value.

```
config system ha
   set standalone-config-sync enable
   set session-pickup enable
   set session-pickup-connectionless enable
   set session-pickup-expectation enable
   set session-pickup-nat enable
   set hbdev 1-M1 50 1-M2 50
end
```

As sessions are forwarded by the routers or load balancers to one of the FortiGate-7040Es, the FGSP synchronizes the sessions to the other FortiGate-7040E. You can log into peer_1 and make configuration changes, which are synchronized to peer_2.

Standalone configuration synchronization

FortiGate-7000E supports configuration synchronization (also called standalone configuration synchronization) for two FortiGate-7000Es. Configuration synchronization means that most configuration changes made to one of the FortiGate-7000Es are automatically synchronized to the other one.

For details about standalone configuration synchronization for FortiOS 6.0, see: Standalone configuration sync.

Use the following command on both FortiGate-7000Es to enable configuration synchronization:

```
config system ha
   set standalone-config-sync enable
end
```

In addition to enabling configuration synchronization, you must set up HA heartbeat connections between the FortiGate-7000Es using the 1-M1, 1-M2, 2-M1, and 2-M2 interfaces. One HA heartbeat connection is required, two are recommended. Use the following command to enable heartbeat configuration for the 1-M1 and 1-M2 interfaces. This command gives both heartbeat interfaces the same priority. You can choose to select different priorities for each heartbeat interface:

```
config system ha
   set hbdev 1-M1 50 1-M2 50
end
```

When you enable configuration synchronization, configure and connect the heartbeat devices, FGCP primary unit selection criteria selects a config sync primary FortiGate-7000E. Normally, the FortiGate-7000E with the highest serial number becomes the config sync primary and the other FortiGate-7000E becomes the config sync secondary.

All configuration changes that you make to the primary are synchronized to the secondary. To avoid synchronization problems, Fortinet recommends making all configuration changes to the primary.

See Limitations on page 108 for a list of limitations of the configuration synchronization feature. Fortinet recommends disabling configuration synchronization once the configurations of the FortiGate-7000Es have been synchronized.

Config sync primary FortiGate-7000E selection

You can use device priority to select one of the FortiGate-7000Es to become the config sync primary. For example, the following command enables configuration synchronization and sets a higher device priority than the default of 128 to make sure that this FortiGate-7000E becomes the primary.

```
config system ha
   set standalone-config-sync enable
   set priority 250
end
```

Settings that are not synchronized

Configuration synchronization does not synchronize settings that identify the FortiGate-7000E to the network. The following settings are not synchronized:

- Transparent mode management IPv4 and IPv6 IP addresses and default gateways.
- All `config system cluster-sync` settings.
- All `config system interface` settings except `vdom`, `vlanid`, `type` and `interface`.
- All `config firewall sniffer` settings.
- All router BFD and BFD6 settings.
- The following BGP settings: `as`, `router-id`, `aggregate-address`, `aggregate-address6`, `neighbor-group`, `neighbor`, `network`, and `network6`.
- The following OSPF settings: `router-id`, `area`, `ospf-interface`, `network`, `neighbor`, and `summary-address`.
- The following OSPF6 settings: `router-id`, `area`, and `ospf6-interface`.
- All RIP settings.
- All policy routing settings.
- All static routing settings.

Limitations

When configuration synchronization is enabled, there are some limitations, including but not limited to the following:

- Configuration synchronization does not support graceful HA firmware upgrades. If you upgrade the firmware of the primary, the secondary also upgrades at the same time, disrupting network traffic. You can avoid traffic interruptions by disabling configuration synchronization and upgrading the firmware of each FortiGate-7000E separately.
- The configuration settings that are synchronized might not match your requirements. The current design and implementation of configuration synchronization is based on requirements from specific customers and might not work for your implementation.
- It can be difficult to control which FortiGate-7000E becomes the config sync primary and the config sync primary can dynamically change without notice. This could result in accidentally changing the configuration of the secondary or overwriting the configuration of the intended primary.

FortiGate-7000E VRRP HA

FortiGate-7000E supports the Virtual Router Redundancy Protocol (VRRP), allowing you to configure VRRP HA between FortiGate-7000E data interfaces. You can also add a FortiGate-7000E data interface to a VRRP domain with other VRRP routers.

To set up a FortiGate-7000E VRRP to provide HA for internet connectivity:

1. Add a virtual VRRP router to the internal interface to the FortiGate-7000E(s) and routers to be in the VRRP domain.
2. Set the VRRP IP address of the domain to the internal network default gateway IP address.
3. Give one of the VRRP domain members the highest priority so it becomes the primary router and give the others lower priorities so they become backup routers.

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

On the GUI you can go to **Network > Interfaces** and right click on the column header and add VRRP to the **Selected Columns** list to see the VRRP status of the data interfaces that are operating as VRRP routers.

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

Operating a FortiGate-7000E

This chapter is a collection of information that you can use when operating your FortiGate-7000E system.

FortiLink support

FortiGate-7000E supports managing FortiSwitch devices over FortiLink. You can manage up to 300 FortiSwitch devices from one FortiGate-7000E.

Use the following command to enable Fortilink support on the GUI and in the CLI:

```
config system global
   set switch-controller enable
end
```

Managed FortiSwitch GUI pages appear under the **WiFi & Switch Controller** GUI menu on all VDOMs except mgmt-vdom.

A FortiGate-7000E manages one or more FortiSwitches through one active FortiLink. The FortiLink can consist of one physical interface or multiple physical interfaces in a LAG. To set up a FortiGate-7000E interface as a FortiLink, from the GUI go to **Network > Interface**, select an interface, and set the **Addressing mode** to **Dedicated to FortiSwitch**.

You can also use the following CLI command to set the 1-C1 interface to be the FortiLink:

```
config system interface
   edit 1-C1
      set auto-auth-extension-device enable
      set fortilink enable
   end
end
```

The FortiGate-7000E has the following FortiLink support limitations:

- The FIM in slot 1 (FIM-01) must be the primary FIM. FortiLink will not work if FIM-02 is the primary FIM.

  In an HA configuration, if the FIM in slot 1 of the primary FortiGate-7000E fails, the secondary FortiGate-7000E becomes the new primary FortiGate-7000E with a functioning FIM in slot 1 and FortiLink support continues after the failover.

- FortiGate-7000E does not support upgrading managed FortiSwitch firmware from the **FortiOS Managed FortiSwitch GUI** page. Instead you must use the FortiGate-7000E CLI or log into the managed FortiSwitch to upgrade managed FortiSwitch firmware.
- You can use any FortiGate-7000E interface as the FortiLink. However, using the M1, M2, and management interfaces is not recommended.

For more information about FortiLink support and managing FortiSwitches, see Switch Controller.

ECMP support

FortiGate-7000E supports most FortiOS IPv4 and IPv6 ECMP functionality. Before setting up an ECMP configuration you need to use the following command to configure the DP processor to operate with VDOM-based session tables:

```
config load-balance setting
   set dp-session-table-type vdom-based
end
```

Once you have enabled VDOM-based session tables, you can enable and configure ECMP as you would for any FortiGate.

VDOM-based session tables

In an ECMP configuration, because of load balancing, return traffic could enter through a different interface than the one it exited from. If this happens, the DP processor operating with default interface-based session tables may not be able to send the return traffic to the FPM that processed the incoming session, causing the return traffic to be dropped. Operating with VDOM-based session tables solves this problem, allowing traffic received on a different interface to be properly identified and sent to the correct FPM .

Enabling VDOM session tables can reduce connections per second (CPS) performance so it should only be enabled if needed to support ECMP. This performance reduction can be more noticeable if the FortiGate-7000E is processing many firewall only sessions. If the FortiGate-7000E is performing content inspection where CPS performance is less important, the performance reduction resulting from enabling VDOM-based session tables may be less noticeable.

IPv4 and IPv6 ECMP load balancing

You can use the following command to configure the IPv4 ECMP load balancing method for a VDOM:

```
config system settings
   set v4-ecmp-mode {source-ip-based | weight-based | source-dest-ip-based}
end
```

With VDOM-based session tables enabled, the FortiGate-7000E supports all IPv4 ECMP load balancing methods supported by FortiOS except usage-based.

See this link for information about how to support IPv6 ECMP load balancing: Technical Tip: ECMP – Load balancing algorithms for IPv4 and IPv6.

Enabling auxiliary session support

When ECMP is enabled, TCP traffic for the same session can exit and enter the FortiGate on different interfaces. To allow this traffic to pass through, FortiOS creates auxiliary sessions. Allowing the creation of auxiliary sessions is handed by the following command:

```
config system settings
   set auxiliary-sessions {disable | enable}
end
```

By default, the `auxiliary-session` option is disabled. This can block some TCP traffic when ECMP is enabled. If this occurs, enabling `auxiliary-session` may solve the problem. For more information, see Technical Tip: Enabling auxiliary session with ECMP or SD-WAN.

ICAP support

You can configure your FortiGate-7000E to use Internet Content Adaptation Protocol (ICAP) to offload processing that would normally take place on the FortiGate-7000E 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-7000E 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 <interface> <interface>
      set dstintf <interface> <interface>
      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-7000E 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 of 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.

Use the information in Mirroring SSL traffic in policies to set up SSL mirroring for your FortiGate-7000E.

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

```
diagnose sniffer packet <interface> 'port 443' -c 50
interfaces=[1-C1/7]
filters=[port 443]
pcap_lookupnet: <interface>: 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
```

VXLAN support

FortiGate-7000E supports terminating VXLAN traffic using VXLAN interfaces. VXLAN traffic cannot be load balanced, so you should use a flow rule similar to the following to send all VXLAN traffic terminated by the FortiGate-7000E to the primary FPM:

```
config load-balance flow-rule
   edit 0
      set status enable
      set ether-type ip
      set protocol 17
      set forward-slot master
      set src-interface <local LAN>
      set dst-l4port 4789-4789
      set comment "vxlan"
   end
```

`dst-l4port` must be set to the VXLAN destination port. The default VXLAN destination port is 4789. You should change the port number range in the flow rule if you change the VXLAN port number.

FortiGate-7000E IPsec load balancing EMAC VLAN interface limitation

On a FortiGate-7000E, because of a DP processor limitation, IPsec VPN load balancing is not supported for sessions received by an EMAC VLAN interface that is not in the same VDOM as the interface that the EMAC VLAN interface has been added to.

The following workarounds are available:

- Change the FortiGate-7000E configuration so that the EMAC VLAN interface is in the same VDOM as the interface that the EMAC VLAN interface is added to (the EMAC VLAN interface is in the same VDOM as its parent interface).

- Disable IPsec VPN load balancing and configure the IPsec phase 1 to send packets to the primary FPM or to a specific FPM. If you have multiple IPsec VPNs, you can achieve some load balancing by configuring different IPsec phase 1 configurations to send packets to different FPMs.

  In addition, for each IPsec phase 1, create a flow rule to forward clear-text traffic from the EMAC VLAN interface to the primary FPM or to a specific FPM. The FPM in the flow rule must match the FPM in the IPsec phase 1 configuration.
- Do not use EMAC VLAN interfaces. For example, you could use standard VLAN interfaces. This may require using an external switch to handle VLAN tagging.

Global option for proxy-based certificate queries

In some cases you may want to be able to send certificate queries using a FortiGate-7000E management interface instead of a data interface. FortiGate-7000E includes the following global command that you can use to enable or disable using a data interface or a system management interface for certificate queries for proxy-based firewall policies.

```
config global
   config system global
      set proxy-cert-use-mgmt-vdom {disable | enable}
   end
```

This option is disabled by default and by default data interfaces are used to send certificate queries for proxy-based firewall policies. Enable this option to send certificate queries for proxy-based firewall policies through the mgmt-vdom VDOM using FortiGate-7000E management interfaces.

Using data interfaces for management traffic

You can set up in-band management connections to all FortiGate-7000E data interfaces by setting up administrative access for the data interface that you want to use to manage the FortiGate-7000E. For in-band management of a transparent mode VDOM, you must also set up the transparent mode management IP address.

Connecting to a data interface for management is the same as connecting to one of the management interfaces. For example, you can log in to the GUI or CLI of the FortiGate-7000E primary FIM.

Administrators with VDOM-level access can log into to their VDOM if they connect to a data interface that is in their VDOM.

In-band management limitations

In-band management has the following limitations:

- In-band management does not support using special port numbers to connect to individual FIMs or FPMs. If you have logged in using an in-band management connection, the special management HTTPS port numbers appear on the Security Fabric dashboard widget when you hover over individual FIMs or FPMs. You can click on an FIM or FPM in the Security Fabric dashboard widget and select **Login to...** to log into the GUI of that FIM or FPM. This action creates an out-of-band management connection by crafting a URL that includes the IP address of the mgmt interface, plus the special HTTPS port number required to connect to that FIM or FPM.
- SNMP in-band management is not supported.

- VRF routes are not applied to outgoing in-band management traffic.
- Changes made on the fly to administrative access settings are not enforced for in-progress in-band management sessions. The changes apply to new in-band sessions only. For example, if an administrator is using SSH for an in-band management connection and you change the SSH administrative port, that in-band management session can continue. Any out-of-band management sessions would need to be restarted with the new port number. New in-band SSH management sessions need to use the new port number. HTTPS access works the same way; however, HTTPS starts new sessions every time you navigate to a new GUI page. So an on the fly change would affect an HTTPS in-band management session whenever the administrator navigates to a new GUI page.

Setting the MTU for a data interface

You can use the following command to change the MTU for a FortiGate-7000E data interface:

```
config system interface
   edit 1B5/1
      set mtu-override enable
      set mtu <value>
   end
```

For the FortiGate-7000E the default `<value>` is 1500 and the range is 256 to 9198.

More management connections than expected for one device

The FortiGate-7000E may show more management-related network activity than most FortiGate devices. This occurs because many management functions are handled independently by each FIM and FPM.

For example, when a FortiGate-7000E first starts up, the FIMs and FPMs perform their DNS lookups. Resulting in more DNS-related traffic during startup than expected for a single device. Once the system is processing data traffic, the amount of management traffic would be proportional to the amount of traffic the system is processing.

More ARP queries than expected for one device - potential issue on large WiFi networks

The FortiGate-7000E sends more ARP queries than expected because each FPM builds its own ARP table to be able to communicate with devices in the same broadcast domain or layer 2 network. This behavior does not cause a problem with most layer 2 networks. However, because the ARP traffic for all of the FPMs comes from the same mac and IP address, on networks with broadcast filtering or ARP suppression, some of the FortiGate-7000E ARP queries and replies may be suppressed. If this happens, FPMs may not be able to build complete ARP tables. An FPM with an incomplete ARP table will not be able to forward sessions to some destinations that it should be able to reach, resulting in dropped sessions.

Broadcast filtering or ARP suppression is commonly used on large WiFi networks to control the amount of ARP traffic on the WiFi network. Dropped FortiGate-7000E sessions have been seen when a FortiGate-7000E is connected to the same broadcast domain as a large WiFi network with ARP suppression.

To resolve this dropped session issue, you can remove broadcast filtering or ARP suppression from the network. If this is not an option, Fortinet recommends that you install a layer 3 device to separate the FortiGate-7000E from the WiFi network broadcast domain. ARP traffic is reduced because the FPMs no longer need to add the addresses of all of the WiFi devices to their ARP tables since they are on a different broadcast domain. The FPMs just need to add the address of the layer 3 device.

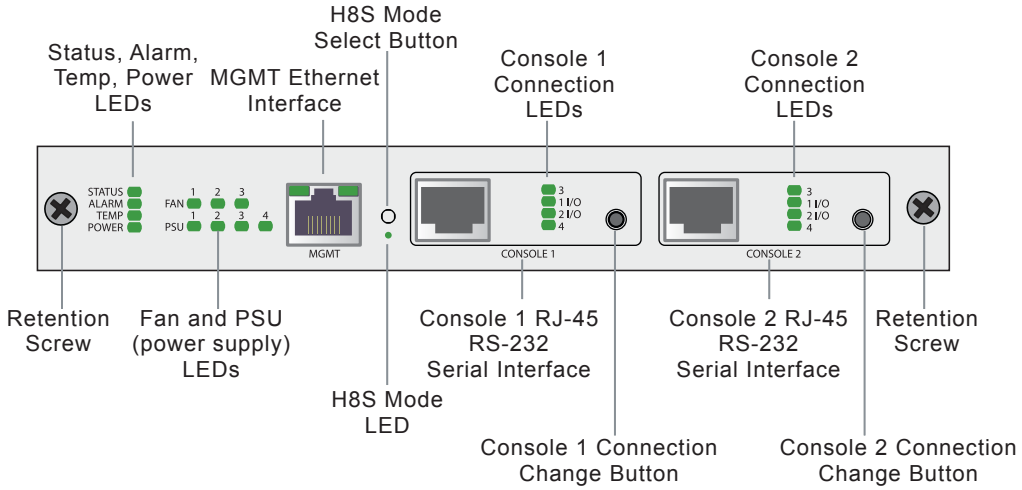
VLAN ID 1 is reserved

When setting up VLANs, do not set the VLAN ID to 1. This VLAN ID is reserved by FortiOS. Any configurations that use a VLAN with VLAN ID = 1 will not work as expected.

Connecting to module CLIs using the System Management Module

All FortiGate-7000E chassis includes a System Management Module (SMM) (also called a shelf manager) on the chassis front panel. See the system guide for your chassis for details about the SMM.

ForiGate-7040E SMM front panel



The SMM 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 SMM 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 SMM 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 SMM 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.

Remote logging for individual FPMs

The FortiGate-7000E supports using VDOM exception functionality to configure different remote logging settings for each FPM. As described in the following sections, you can:

- Configure individual FPMs to send log messages to different FortiAnalyzers or syslog servers.
- Configure VDOMs on individual FPMs to send log messages to different FortiAnalyzers or syslog servers.

This configuration is only supported for `fortianalyzer` and `syslogd` and not for `fortianalyzer2`, `fortianalyzer3`, `fortianalyzer-cloud`, `syslogd2`, `syslogd3`, and `syslogd4`.

When you have completed the VDOM exception configurations described in this section, the FIMs and FPMs will have different logging configurations. In addition, some configurations that are affected by the logging configuration (for example, DLP content archiving) will be different on some modules. Because of this, using the various methods available to check for synchronization between modules will show that the configurations of the modules are not synchronized. The FortiGate-7000E will continue to operate normally even with these configuration synchronization issues.

Some VDOM exception options not supported in HA mode

When a FortiGate-7000E is operating in FGCP HA mode, only the following `vdom-exception` options can be configured:

```
log.fortianalyzer.setting
log.fortianalzer.override-setting
log.syslogd.setting
log.syslogd.override-setting
```

The CLI returns an error message if you attempt to configure a `vdom-exception` that is not configurable in HA mode.

Also in HA mode, only the primary FortiGate-7000E can send log messages from individual VDOMs because only the data interfaces on the primary FortiGate-7000E are active.

Configuring individual FPMs to send logs to different FortiAnalyzers

The following steps show how to configure the two FPMs in a FortiGate-7040E to send log messages to different FortiAnalyzers. The FPMs connect to their FortiAnalyzers through the FortiGate-7000E management interface. This procedure assumes you have the following three FortiAnalyzers:

FortiAnalyzer IP address	Intended use
172.25.176.10	The FIMs send log messages to this FortiAnalyzer.
172.25.176.100	The FPM in slot 3 sends log messages to this FortiAnalyzer.
172.25.176.110	The FPM in slot 4 sends log messages to this FortiAnalyzer.

This procedure involves creating a FortiAnalyzer configuration template on the primary FIM that is synchronized to the FPMs. You then log into each FPM and change the FortiAnalyzer server IP address to the address of the FortiAnalyzer that the FPM should send log messages to.

This configuration is only supported for `fortianalyzer` and not for `fortianalyzer2`, `fortianalyzer3`, and `fortianalyzer-cloud`.

1. Log into the primary FIM CLI using the FortiGate-7040E management IP address.
2. Create a FortiAnalyzer configuration template on the primary FIM.

```
config global
   config log fortianalyzer setting
      set status enable
      set server 172.25.176.10
      set upload-option realtime
   end
```

This configuration will be synchronized to all of the FIMs and FPMs.

The FortiAnalyzer VDOM exception configuration requires `upload-option` to be set to `realtime`.

3. Enter the following command to prevent the FortiGate-7040E from synchronizing FortiAnalyzer settings between FIMs and FPMs:

```
config system vdom-exception
   edit 1
      set object log.fortianalyzer.setting
   end
```

4. Log into the CLI of the FPM in slot 3:

   For example, you can start a new SSH connection using the special management port for slot 3:

```
ssh <management-ip>:2203
```

   Or you can use the following command from the global primary FIM CLI:

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

FortiOS will log you out of the CLI of the FPM in slot 3 in less than 60 seconds. You should have enough time to change the FortiAnalyzer server IP address as described in the next step, but not much else. If you run out of time on your first attempt, you can keep trying until you succeed.

5. Change the FortiAnalyzer server IP address:

```
config global
   config log fortianalyzer setting
      set server 172.25.176.100
   end
```

   You should see messages similar to the following on the CLI:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
     out of sync for a while.
The Serial Number for FortiAnalyzer is not entered.
In order to verify identity of FortiAnalyzer serial number is needed.
If serial number is not set, connection will be set as unverified and
access to local config and files will be accessible only with user name/password.
FortiGate can establish a connection to obtain the serial number now.Do you want to try
     to connect now? (y/n)y
```

If `upload-option` is not set to `realtime`, messages similar to the following appear and your configuration change will not be saved:

```
Please change configuration on FIMs. Changing configuration on FPMs
     may cause confsync out of sync for a while.
Can only set upload option to real-time mode when Security Fabric is
     enabled.
object set operator error, -39 discard the setting
Command fail. Return code -39
```

6. Enter Y to confirm the serial number. Messages similar to the following should appear:

```
Obtained serial number from X509 certificate of Fortianalyzer is: <serial>
Serial number from certificate MUST be the same as serial number observed in
     Fortianalyzer.
If these two serial numbers don't match, connection will be dropped.
Please make sure the serial numbers are matching.
In case that Fortianalyzer is using a third-party certificate, certificate verification
     must be disabled.
Do you confirm that this is the correct serial number? (y/n)y
```

7. Enter Y to confirm the serial number.
8. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

9. Log into the CLI of the FPM in slot 4.
10. Change the FortiAnalyzer server IP address:

```
config global
   config log fortianalyzer setting
      set server 172.25.176.110
   end
```

When you change the FortiAnalyzer server IP address, messages appear like they did when you were logged into the FPM in slot 3 and you can confirm the FortiAnalyzer serial number.

11. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

Configuring VDOMs on individual FPMs to send logs to different FortiAnalyzers

The following steps describe how to override the global FortiAnalyzer configuration for individual VDOMs on individual FPMs. The example shows how to configure the root VDOMs on the each of the FPMs in a FortiGate-7040E to send log messages to different FortiAnalyzers. Each root VDOM connects to FortiAnalyzer through a root VDOM data interface. This procedure assumes you have the following two FortiAnalyzers:

FortiAnalyzer IP address	Intended use
172.25.176.120	The root VDOM on the FPM in slot 3 sends log messages to this FortiAnalyzer.
172.25.176.130	The root VDOM on the FPM in slot 4 sends log messages to this FortiAnalyzer.

This configuration is only supported for `fortianalyzer` and not for `fortianalyzer2`, `fortianalyzer3`, and `fortianalyzer-cloud`.

1. Log into the primary FIM CLI using the FortiGate-7040E management IP address.
2. Use the following command to prevent the FortiGate-7040E from synchronizing FortiAnalyzer override settings between FPMs:

```
config global
   config system vdom-exception
      edit 1
         set object log.fortianalyzer.override-setting
      end
   end
```

3. Log into the CLI of the FPM in slot 3:

   For example you can start a new SSH connection using the special management port for slot 3:

   `ssh <management-ip>:2203`

   Or you can use the following command from the global primary FIM CLI:

   `execute load-balance slot manage 3`

The system will log you out of the CLI of the FPM in slot 3 in less than 60 seconds. You should have enough time to complete the following steps. If you run out of time on your first attempt, you can keep trying until you succeed.

4. Access the root VDOM of the FPM in slot 3 and enable overriding the FortiAnalyzer configuration for the root VDOM.

```
config vdom
  edit root
    config log setting
      set faz-override enable
    end
```

A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
    out of sync for a while.
```

5. Configure FortiAnalyzer override to send log messages to a FortiAnalyzer with IP address 172.25.176.120:

```
config log fortianalyzer override-setting
  set status enable
  set server 172.25.176.120
end
```

You should see messages similar to the following on the CLI:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
    out of sync for a while.
The Serial Number for FortiAnalyzer is not entered.
In order to verify identity of FortiAnalyzer serial number is needed.
If serial number is not set, connection will be set as unverified and
access to local config and files will be accessible only with user name/password.
FortiGate can establish a connection to obtain the serial number now.Do you want to try
    to connect now? (y/n)y
```

6. Enter Y to confirm the serial number. Messages similar to the following should appear:

```
Obtained serial number from X509 certificate of Fortianalyzer is: <serial>
Serial number from certificate MUST be the same as serial number observed in
    Fortianalyzer.
If these two serial numbers don't match, connection will be dropped.
Please make sure the serial numbers are matching.
In case that Fortianalyzer is using a third-party certificate, certificate verification
    must be disabled.
Do you confirm that this is the correct serial number? (y/n)y
```

7. Enter Y to confirm the serial number.
8. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute
9. Log into the CLI of the FPM in slot 4.
10. Access the root VDOM of the FPM in slot 4 and enable overriding the FortiAnalyzer configuration for the root VDOM.

```
config vdom
  edit root
    config log setting
      set faz-override enable
    end
```

A message similar to the following appears; which you can ignore:

```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
    out of sync for a while.
```

11. Configure FortiAnalyzer override to send log messages to a FortiAnalyzer with IP address 172.25.176.130:

```
config log fortianalyzer override-setting
  set status enable
  set server 172.25.176.130
end
```

Messages appear like they did when you were logged into the FPM in slot 3 and you can confirm the FortiAnalyzer serial number.

12. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

Configuring individual FPMs to send logs to different syslog servers

The following steps show how to configure the two FPMs in a FortiGate-7040E to send log messages to different syslog servers. The FPMs connect to the syslog servers through the FortiGate-7000E management interface. This procedure assumes you have the following three syslog servers:

syslog server IP address	Intended use
172.25.176.20	The FIMs send log messages to this syslog server.
172.25.176.200	The FPM in slot 3 sends log messages to this syslog server.
172.25.176.210	The FPM in slot 4 sends log messages to this syslog server.

This procedure involves creating a syslog configuration template on the primary FIM that is synchronized to the FPMs. You then log into each FPM and change the syslog server IP address to the address of the syslog server that the FPM should send log messages to.

This configuration is only supported for `syslogd` and not for `syslogd2`, `syslogd3`, and `syslogd4`.

1. Log into the primary FIM CLI using the FortiGate-7040E management IP address.
2. Create a syslog configuration template on the primary FIM.

```
config global
   config log syslogd setting
      set status enable
      set server 172.25.176.20
   end
```

   This configuration will be synchronized to all of the FIMs and FPMs.
3. Enter the following command to prevent the FortiGate-7040E from synchronizing syslog settings between FIMs and FPMs:

```
config system vdom-exception
   edit 1
      set object log.syslogd.setting
   end
```

4. Log into the CLI of the FPM in slot 3:

   For example, you can start a new SSH connection using the special management port for slot 3:

```
ssh <management-ip>:2203
```

   Or you can use the following command from the global primary FIM CLI:

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

FortiOS will log you out of the CLI of the FPM in slot 3 in less than 60 seconds. You should have enough time to change the syslog server IP address as described in the next step, but not much else. If you run out of time on your first attempt, you can keep trying until you succeed.

5. Change the syslog server IP address:
```
config global
   config log syslogd setting
      set server 172.25.176.200
   end
```
A message similar to the following appears; which you can ignore:
```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
     out of sync for a while.
```
6. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.
7. Log into the CLI of the FPM in slot 4.
8. Change the syslog server IP address:
```
config global
   config log syslogd setting
      set server 172.25.176.210
   end
```
A message similar to the following appears; which you can ignore:
```
Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
     out of sync for a while.
```
9. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

Configuring VDOMs on individual FPMs to send logs to different syslog servers

The following steps describe how to override the global syslog configuration for individual VDOMs on individual FPMs. The example shows how to configure the root VDOMs on the each of the FPMs in a FortiGate-7040E to send log messages to different sylog servers. Each root VDOM connects to a syslog server through a root VDOM data interface. This procedure assumes you have the following two syslog servers:

syslog server IP address	Intended use
172.25.176.220	The root VDOM on the FPM in slot 3 sends log messages to this syslog server.
172.25.176.230	The root VDOM on the FPM in slot 4 sends log messages to this syslog server.

This configuration is only supported for `syslogd` and not for `syslogd2`, `syslogd3`, and `syslogd4`.

1. Log into the primary FIM CLI using the FortiGate-7040E management IP address.
2. Use the following command to prevent the FortiGate-7040E from synchronizing syslog override settings between FPMs:
```
config global
   config system vdom-exception
```

```
    edit 1
      set object log.syslogd.override-setting
    end
  end
```

3. Log into the CLI of the FPM in slot 3:

   For example you can start a new SSH connection using the special management port for slot 3:

   ```
   ssh <management-ip>:2203
   ```

   Or you can use the following command from the global primary FIM CLI:

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

   The system will log you out of the CLI of the FPM in slot 3 in less than 60 seconds. You should have enough time to complete the following steps. If you run out of time on your first attempt, you can keep trying until you succeed.

4. Access the root VDOM of the FPM in slot 3 and enable overriding the syslog configuration for the root VDOM.

   ```
   config vdom
     edit root
       config log setting
         set syslog-override enable
       end
   ```

   A message similar to the following appears; which you can ignore:

   ```
   Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
       out of sync for a while.
   ```

5. Configure syslog override to send log messages to a syslog server with IP address 172.25.176.220:

   ```
   config log syslogd override-setting
     set status enable
     set server 172.25.176.220
   end
   ```

   A message similar to the following appears; which you can ignore:

   ```
   Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
       out of sync for a while.
   ```

6. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

7. Access the root VDOM of the FPM in slot 4 and enable overriding the syslog configuration for the root VDOM.

   ```
   config vdom
     edit root
       config log setting
         set syslog-override enable
       end
   ```

   A message similar to the following appears; which you can ignore:

   ```
   Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
       out of sync for a while.
   ```

8. Configure FortiAnalyzer override to send log messages to a FortiAnalyzer with IP address 172.25.176.130:

   ```
   config log syslogd override-setting
     set status enable
     set server 172.25.176.230
   end
   ```

   A message similar to the following appears; which you can ignore:

   ```
   Please change configuration on FIMs. Changing configuration on FPMs may cause confsync
       out of sync for a while.
   ```

9. Use the `exit` command to log out of the FPM CLI. Otherwise you are logged out of the FPM CLI in less than a minute.

Firmware upgrade basics

All of the FIMs and FPMs in your FortiGate-7000E system run the same firmware image. You upgrade the firmware from the primary FIM GUI or CLI just as you would any FortiGate product.

You can perform a graceful firmware upgrade of a FortiGate-7000E FGCP HA cluster by setting `upgrade-mode` to `uninterruptible` and enabling `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

Upgrading the firmware of a standalone FortiGate-7000E, or FortiGate-7000E HA cluster with `upgrade-mode` set to `simultaneous` interrupts traffic because the firmware running on the FIMs and FPMs upgrades in one step. These firmware upgrades should be done during a quiet time because traffic will be interrupted during the upgrade process.

A firmware upgrade takes a few minutes, depending on the number of FIMs and FPMs in your FortiGate-7000E system. Some firmware upgrades may take longer depending on factors such as the size of the configuration.

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-7000E configuration.

To make sure a FortiGate-7000E firmware upgrade is successful, before starting the upgrade Fortinet recommends you use health checking to make sure the FIMs and FPMs are all synchronized and operating as expected.

If you are following a multi-step upgrade path, you should re-do health checking after each upgrade step to make sure all components are synchronized before the next step.

You should also perform a final round of health checking after the firmware upgrade process is complete.

For recommended health checking commands, see the following Fortinet community article:

Technical Tip: FortiGate-6000/7000 Chassis health check commands.

Fortinet recommends that you review the services provided by your FortiGate-7000E 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.

Verifying that a firmware upgrade is successful

After a FortiGate-7000E 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 System Information dashboard widget or by using the `get system status` command.
2. Confirm that the FortiGate-7000E is synchronized.
   Go to **Monitor > Configuration Sync Monitor** to verify the configuration status of the FIMs and FPMs. 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.
3. Optionally, you can also log into the other FIM and FPMs, and in the same way confirm that they are also running the expected firmware version and are synchronized.

Installing firmware on individual FIMs or 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-7000E front panel SMM 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-7000E 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-7000E 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-7000E. These procedures also work for FIMs or FPMs in the primary FortiGate-7000E in an HA configuration. To upgrade firmware on an FIM or FPM in the secondary FortiGate-7000E in an HA configuration, you should either remove the secondary FortiGate-7000E from the HA configuration or cause a failover so that the secondary FortiGate-7000E becomes the primary FortiGate-7000E.

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

Upgrading the firmware on an individual FIM

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

To upgrade the firmware on a individual FIM from the GUI

1. Connect to the FIM GUI using the SLBC management IP address and the special management port number for that FIM. For example, for the FIM in slot 2, browse to https://<SLBC-management-ip>:44302.
2. Start a normal firmware upgrade. For example,
   a. Go to **System > Firmware** and select **Browse** to select the firmware file to install.
   b. Follow the prompts to select the firmware file, save the configuration, and upload the firmware file to the FPM.
3. After 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.
4. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration of the FIM has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.
   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 at https://support.fortinet.com.
   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 Configuration Sync Monitor will temporarily show that it is not synchronized.

To upgrade the firmware on a individual FIM from the CLI using TFTP

1. Put a copy of the firmware file on a TFTP server that is accessible from the SLBC management interface.
2. Connect to the FIM CLI by using an SSH client. For example, to connect to the CLI of the FIM in slot 2, connect to <SLBC-management-ip>:2201.
3. Enter the following command to upload the firmware file to the FIM:
   `execute upload image tftp <firmware-filename> comment <tftp-server-ip-address>`
4. After 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.
5. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration of the FIM has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.
   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 at https://support.fortinet.com.
   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 Configuration Sync Monitor will temporarily show that it is not synchronized.

Upgrading the firmware on an individual FPM

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 slot containing the FPM to be upgraded.
2. Log in to the FPM GUI or CLI using its special port number.
   To upgrade the firmware on the FPM in slot 3 from the GUI:
   a. Connect to the FPM GUI by browsing to https://<SLBC-management-ip>:44303.
   b. Go to **System > Firmware** and select **Browse** to select the firmware file to install.
   c. Follow the prompts to select the firmware file, save the configuration, and upload the firmware file to the FPM.
   To upgrade the firmware on an FPM from the CLI using TFTP see Installing FPM firmware from the BIOS after a reboot.
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. Use the diagnose sys confsync status | grep in_sy to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of that FIM or FPM is synchronized.
   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 at https://support.fortinet.com.
   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 Configuration Sync Monitor 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.

Installing FIM firmware from the BIOS after a reboot

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-7000E front panel System Management Module console port. From the console session, the procedure describes how to restart the FIM, interrupt 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 interfaces that are part of the LAG from the switch. This includes MGMT interfaces from both FIMs.
3. Using the console cable supplied with your FortiGate-7000E, connect the SMM Console 1 port on the FortiGate-7000E to the USB 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-7000E 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 FIM CLI using the `get system status` command.
16. Use the `diagnose sys confsync status | grep in_sy` command to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the FIM or FPM is synchronized.

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 at https://support.fortinet.com.

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 Configuration Sync Monitor will temporarily show that it is not synchronized.

Installing FPM firmware from the BIOS after a reboot

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-7000E front panel SMM 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-7000E 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. When you set up the FPM TFTP settings below, you select the FIM that can connect to the TFTP server. 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 interfaces that are part of the LAG from the switch. This includes MGMT interfaces from both FIMs
4. Using the console cable supplied with your FortiGate-7000E, connect the SMM Console 1 port on the FortiGate-7000E to the USB 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`: FIM01 (the FIM that can communicate with the TFTP server).

    `[D]: Set DHCP mode`: Disabled.

    `[I]: Set local IP address`: The IP address of the MGMT interface of the selected FIM that you want to use to connect to the TFTP server. This address must not be the same as the FortiGate-7000E 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. Enter the `diagnose sys confsync status | grep in_sy` command to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

    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 at https://support.fortinet.com.

    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 Configuration Sync Monitor 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.

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

```
FIM04E3E16000010, Primary, uptime=69398.91, priority=1, slot_id=1:1, idx=0, flag=0x0, in_sync=1
...
```

You can also verify synchronization status from the primary FIM Configuration Sync Monitor.

To re-synchronize the FortiGate-7000E, 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 Configuration Sync Monitor or using the `diagnose sys confsync status | grep in_sy` command.

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-7000Es or just operating a standalone FortiGate-7000E.

Replacing a failed module in a standalone FortiGate-7000E

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.

   If the firmware on the new module is much older than the firmware running on the FortiGate-7000E, you may have to manually upgrade the new module to the current firmware.
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 Firmware upgrade basics on page 126.
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-7000E 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.

If the firmware on the new module is much older than the firmware running on the FortiGate-7000E, you may have to manually upgrade the new module to the current firmware.

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 at https://support.fortinet.com.

Resolving FIM or FPM boot device I/O errors

If an FIM or FPM has boot device I/O errors, messages similar to the following appear during console sessions with the module:

```
EXT2-fs (sda1): previous I/O error to superblock detected
EXT2-fs (sda3): previous I/O error to superblock detected
```

If you see boot device I/O errors similar to these, you should contact Fortinet Support (https://support.fortinet.com) for assistance with finding the underlying cause of these errors.

Once the underlying cause is determined and resolved, you use BIOS commands to reformat and restore the affected boot device as described in the following sections.

Formatting an FIM boot device and installing new firmware

You can use the following steps to format an FIM boot device and install new firmware from a TFTP server.

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.
3. Using the console cable supplied with your FortiGate-7000E, connect the SMM Console 1 port on the FortiGate-7000E to the USB 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 format the FIM boot disk, press F.
11. Press Y to confirm that you want to erase all data on the boot disk and format it.

    When the formatting is complete the FIM restarts.
12. Follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.
13. To set up the TFTP configuration, press C.
14. 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-7000E 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.
15. To quit this menu, press Q.
16. 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.

17. 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.
18. 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.
19. Enter the `diagnose sys confsync status | grep in_sy` command to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

    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 at https://support.fortinet.com.

    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 Configuration Sync Monitor will temporarily show that it is not synchronized.

Formatting an FPM boot device and installing new firmware

You can use the following steps to format an FPM boot device and install new firmware from a TFTP server.

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-7000E 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. When you set up the FPM TFTP settings below, you select the FIM that can connect to the TFTP server. 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 interfaces that are part of the LAG from the switch. This includes MGMT interfaces from both FIMs
4. Using the console cable supplied with your FortiGate-7000E, connect the SMM Console 1 port on the FortiGate-7000E to the USB 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 format the FPM boot disk, press F.
12. Press Y to confirm that you want to erase all data on the boot disk and format it.

    When the formatting is complete the FPM restarts.
13. Follow the boot process in the terminal session, and press any key when prompted to interrupt the boot process.

14. To set up the TFTP configuration, press C.
15. Use the BIOS menu to set the following. Change settings only if required.

    `[P]: Set image download port`: FIM01 (the FIM that can communicate with the TFTP server).

    `[D]: Set DHCP mode`: Disabled.

    `[I]: Set local IP address`: The IP address of the MGMT interface of the selected FIM that you want to use to connect to the TFTP server. This address must not be the same as the FortiGate-7000E 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.
16. To quit this menu, press Q.
17. 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.
18. 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.
19. 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.
20. Enter the `diagnose sys confsync status | grep in_sy` command to verify that the configuration has been synchronized. The field `in_sync=1` indicates that the configurations of the FIMs and FPMs are synchronized.

    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 at https://support.fortinet.com.

    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 Configuration Sync Monitor will temporarily show that it is not synchronized.
21. 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.

Failover in a standalone FortiGate-7000E

A FortiGate-7000E 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 primary. 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, traffic will continue to be received by the other FIM.

Adjusting global DP2 timers

This section describes the global DP2 timers that you can adjust from the CLI. These timers affect the operation of the FortiGate-7000E DP2 processor.

```
config global
   config system global
      set dp-fragment-timer <timer>
      set dp-pinhole-timer <timer>
      set dp-tcp-normal-timer <timer>
      set dp-udp-idle-timer <timer>
   end
```

`dp-fragment-timer` the time to wait for the next fragment of a fragmented packet. The range is 1 to 65535 seconds. The default is 120 seconds. See Load balancing TCP, UDP, and ICMP sessions with fragmented packets on page 53.

`dp-pinhole-timer` the time to wait to close a pinhole if no more matching traffic that would use the pinhole is received by the DP2 processor. The range is 30 to 120 seconds. The default is 120 seconds.

`dp-tcp-normal-timer` the time to wait before the DP2 processor closes an idle TCP session. The range is 1 to 65535 seconds. The default is 3605 seconds. Some FortiGate-7000E implementations may need to increase this timer if TCP or UDP sessions with NAT enabled are expected to or found to be idle for more than 3605 seconds.

`dp-udp-idle-timer` the time to wait before the DP2 processor closes an idle UDP session. The range is 1 to 86400 seconds. The default is 0, which means the DP2 processor uses the UDP idle timer set by the `udp-idle-timer` option of the `config system global` command.

Resetting to factory defaults

At any time during the configuration process, if you run into problems, you can reset the FortiGate-7000E to factory defaults and start over. From the primary FIM CLI enter:

```
config global
   execute factoryreset
```

Restarting the FortiGate-7000E

To restart all of the modules in a FortiGate-7000E, 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.

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-7000E 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-7000E `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:"
```

FortiGate-7000E config CLI commands

This chapter describes the following FortiGate-7000E 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 {<protocol-number> | 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 {<protocol-number> | 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`. You can specify any protocol number or you can use the following keywords to select common protocols.

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

The default priority is 5.

comment <text>

Optionally add a comment that describes the flow rule.

config load-balance setting

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

```
config load-balance setting
   set slbc-mgmt-intf {mgmt1 | mgmt2 | mgmt3)
   set max-miss-heartbeats <heartbeats>
   set max-miss-mgmt-heartbeats <heartbeats>
   set weighted-load-balance {disable | enable}
   set gtp-load-balance {disable | enable}
   set pfcp-load-balance {disable | enable}
   set sslvpn-load-balance {disable | enable}
   set dp-fragment-session {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 sw-load-distribution-method {src-dst-ip | 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 {intf-vlan-based | vdom-based}
   set nat-source-port {chassis-slots | enabled-slots}
      config workers
         edit <slot>
            set status {disable | enable}
            set weight <weight>
         end
```

slbc-mgmt-intf mgmt

Selects the interface used for management connections. For the FortiGate-7000E, this option is always set to `mgmt` and cannot be changed. The IP address of this interface becomes the IP address used to enable management access to individual FIMs or FPMs using special administration ports as described in Special management port numbers on page 44. To manage individual FIMs or FPMs, this interface must be connected to a network.

To enable using the special management port numbers to connect to individual FIMs and FPMs, the mgmt interface must be connected to a network, have a valid IP address, and have management or administrative access enabled. To block access to the special management port numbers, disconnect the mgmt interface from a network, configure the mgmt interface with an invalid IP address, or disable management or administrative access for the mgmt interface.

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.

gtp-load-balance {disable | enable}

Enable or disable GTP-U load balancing. For more information, see Enabling GTP load balancing on page 49.

pfcp-load-balance {disable | enable}

Enable or disable PFCP user plane load balancing. For more information, see PFCP load balancing on page 51.

set sslvpn-load-balance {disable | enable}

Enable or disable SSL VPN load balancing. For more information, see SSL VPN load balancing on page 59.

dp-fragment-session {disable | enable}

Enable or disable efficient DP2 load balancing of TCP, UDP, and ICMP sessions with fragmented packets. The option is disabled by default.

For more information, see Load balancing TCP, UDP, and ICMP sessions with fragmented packets on page 53.

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 by the DP2 processor 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.

sw-load-distribution-method {src-dst-ip | src-dst-ip-sport-dport}

Configure the load distribution method used by the Internal Switch Fabric (ISF). The default setting is `src-dst-ip-sport-dport`.

To support load balancing sessions with fragmented packets, set s`w-load-distribution-method` to `src-dst-ip`. For more information, see Load balancing TCP, UDP, and ICMP sessions with fragmented packets on page 53.

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 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 {intf-vlan-based | vdom-based}

Change DP processing load balancing mode:

`dp-session-table-type` is the default value and should be used in all cases unless the FortiGate-7000E will support ECMP.

`vdom-based` should only be selected to support ECMP. Enabling VDOM session tables can reduce connections per second (CPS) performance so it should only be enabled if needed to support ECMP. This performance reduction can be more noticeable if the FortiGate-7000E is processing many firewall only sessions. For more information, see ECMP support on page 111.

set nat-source-port {chassis-slots | enabled-slots}

Change SNAT port partitioning behavior. For more information, see Controlling SNAT port partitioning behavior on page 56.

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 <slot>
      set status enable
      set weight 5
   end
```

FortiGate-7000E execute CLI commands

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

execute factoryreset-shutdown

You can use this command to reset the configuration of the FortiGate-7000E FIMs and FPMs before shutting the system down. This command is normally used in preparation for resetting and shutting down a FortiGate-7000E.

execute ha manage <id>

In an HA configuration, use this command to log in to the primary FIM of the secondary FortiGate-7000E.

`<id>` is the ID of the secondary FortiGate-7000E. Usually the primary FortiGate-7000E ID is 0 and the secondary ID is 1. You can enter the ? to see the list of IDs that you can connect to.

After you have logged in, you can manage the secondary FortiGate-7000E from the primary FIM or you can use the `execute load-balance slot manage` command to connect to the other FIM and the FPMs in the secondary FortiGate-7000E.

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

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

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

To disconnect the other SMM console, you can log into the SMM 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 SMM 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 SMM console session from the FIM CLI without having to log into the SMM CLI.

execute load-balance console-mgmt info

This command shows whether the SMM console disconnect command is enabled or disabled and also shows which modules the SMM 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-7000E, including a license for extra VDOMs and FortiClient licenses.

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

Reset FortiClient and VDOM licenses added to this FortiGate-7000E to factory defaults.

Specify `crypto-key` to re-generate crypto keys that are generated when the FortiGate-7000E first starts up.

Use `all` to reset all licenses and crypto keys.

Resetting licenses and crypto keys doesn't restart the FortiGate-7000E.

execute set-next-reboot rollback

You can use the following command to change the firmware image that all of the FIMs and FPMs load the next time the FortiGate-7000E starts up.

```
execute set-next-reboot rollback
```

This command causes each component to select the firmware image stored on its non-active partition the next time the system starts up. The new command replaces the need to log into each component CLI and running the `execute set-next-reboot {primary | secondary}` command.

You can install firmware on the backup partition of a FIM of FPM using the `execute restore secondary-image` command or from the BIOS.

execute load-balance slot manage <slot>

Log into the CLI of an individual FIM or FPM. Use `<slot>` to specify the FIM or FPM slot number.

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 original 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 primary FIM 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.

execute load-balance slot set-primary-worker <slot>

Force an FPM to always be the primary FPM, `<slot>` is the FPM slot number.

The change takes place right away and all new primary FPM sessions are sent to the new primary FPM. Sessions that had been processed by the former primary FPM do not switch over, but continue to be processed by the former primary FPM.

This command is most often used for troubleshooting or testing. Since the command does not change the configuration, if the FortiGate-7000E restarts, the usual primary FPM selection process occurs.

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-7000E 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 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 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 FortiGate-7000E 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-7000E 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.

```
show full-configuration
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 primary blade"
    next
    edit 18
        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 primary blade"
    next
    edit 19
        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 primary blade"
    next
    edit 20
        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
    edit 21
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 8805-8805
        set action forward
        set forward-slot master
        set priority 5
        set comment "pfcp to primary blade"
    next
    edit 22
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4784-4784
        set action forward
        set forward-slot master
        set priority 5
        set comment "Flow Rule for Multihop BFD"
    next
end
```

www.fortinet.com