FortiGate-6000 and FortiGate-7000 - Release Notes

Version v6.0.4 Build 8405

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

August 27, 2019
FortiGate-6000 and FortiGate-7000 v6.0.4 Build 8405 Release Notes
01-604-576425-20190827

TABLE OF CONTENTS

Change log

Date	Change description
August 27, 2019	Added more information to Common vulnerabilities and exposures on page 42.
August 15, 2019	Updated for build 8405, a new bug fix release of FortiGate-6000 and FortiGate-7000 for FortiOS 6.0.4. New sections: Upgrading a FortiGate-6000 or FortiGate-7000 HA configuration on page 37 and Resolved issues for build 8405 on page 41.
July 26, 2019	Updated for build 8385, a new bug fix release of FortiGate-6000 and FortiGate-7000 for FortiOS 6.0.4. New section: Resolved issues for build 8385 on page 42.
July 5, 2019	New section: FGSP session synchronization on page 10. Changes to FGCP session synchronization options on page 8 and FGSP session synchronization on page 10.
June 21, 2019	New sections: Default Security Fabric configuration on page 13 and Maximum values on page 40.
April 30, 2019	Minor changes.
April 29, 2019	Minor changes.
April 26, 2019	Minor changes.
April 25, 2019	Initial version (for build 6145).

FortiGate-6000 and FortiGate-7000 v6.0.4 release notes

This document provides the following information for FortiGate-6000 and FortiGate-7000 v6.0.4 build 8405:

Supported models

FortiGate-6000 v6.0.4 build 8405 supports the following models:

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

FortiGate-7000 v6.0.4 build 8405 supports all FortiGate-7030E, 7040E, and 7060E models and configurations.

What's new in FortiGate-6000 and FortiGate-7000 v6.0.4 build 8405

FortiGate-6000 and FortiGate-7000 v6.0.4 build 8405 includes the bug fixes described inResolved issues for build 8405 on page 41 and Resolved issues for build 8385 on page 42. The first released build of FortiGate-6000 and FortiGate-7000 v6.0.4 was build 6145.

The following new features have been added to FortiGate-6000 and FortiGate-7000 v6.0.4 build 8405:

- Diagnose debug flow trace output improvements.
- New diagnose command to show how the DP processor will load balance a session.
- Enabling or disabling synchronizing connectionless sessions.
- ICMP traffic can now be load balanced.
- FortiGate Session Life Support Protocol (FGSP) support.
- The report produced by the `execute tac report` command now includes more information, including new information about SLBC operations.

Diagnose debug flow trace output improvements

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

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

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

```
diagnose debug enable
[FPC02]  id=20085 trace_id=2 func=resolve_ip6_tuple_fast line=4190 msg="vd-vlan:0 received a packet(proto=6,
3ff5::100:10001->4ff5::28:80) from vlan-port1."
[FPC02]  id=20085 trace_id=2 func=resolve_ip6_tuple line=4307 msg="allocate a new session-000f00fb"
[FPC02]  id=20085 trace_id=2 func=vf_ip6_route_input line=1125 msg="find a route: gw-4ff5::28 via vlan-port2
err 0 flags 01000001"
[FPC02]  id=20085 trace_id=2 func=fw6_forward_handler line=345 msg="Check policy between vlan-port1 -> vlan-
port2"
```

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

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

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

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

Show how the DP processor will load balance a session

You can use the following command to display the FPC or FPM slot that the DP 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 slot 8 by the DP processor.

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

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

FGCP session synchronization options

FortiGate-6000 and FortiGate-7000 platforms now support the following FGCP session synchronization options.

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

The `session-pickup-connectionless` option is new in FortiOS 6.0.4. In FortiOS 5.6, enabling `session-pickup` synchronized TCP, SCTP and connectionless (UDP, ICMP, and so on) sessions. In FortiOS 6.0.4, `session-pickup` only synchronizes TCP and SCTP sessions.

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`.

If you have enabled `session-pickup` for FortiOS 5.6, after upgrading to 6.0.4 if you want to continue synchronizing connectionless sessions, you have to manually enable `session-pickup-connectionless`.

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

The `session-pickup-delay` option does not currently work for IPv6 TCP traffic. This known issue (553996) will be fixed in a future firmware version.

The `inter-cluster-session-sync` option is supported only for inter-cluster session synchronization between FGCP clusters.

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 sessions are sent to the primary (master) FPC or FPM. As a result, ICMP sessions are handled in the same way as in previous releases.

If you want to load balance ICMP sessions to multiple FPCs or 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.

Two additional load balance setting options are also visible in this release: `dp-keep-assist-sessions` cannot be changed and `dp-session-table-type` will be supported in a future version. For FortiOS 6.0.4, `dp-session-table-type` must be set to `intf-vlan-based` (the default value).

FGSP support

FortiGate-6000 and FortiGate-7000 for FortiOS 6.0.4 supports FortiGate Session Life Support Protocol (FGSP) HA (also called standalone session sync). FGSP is supported for up to four FortiGate-6000s or FortiGate-7000s. All of the FortiGates in the FGSP cluster must be the same model. For details about FGSP for FortiOS 6.0, see: FGSP.

FortiGate-6000 and FortiGate-7000 FGSP support has the following limitations:

- Configuration synchronization is currently not supported, you must configure all of the devices in the FGSP cluster separately or use FortiManager to keep key parts of the configuration, such as security policies, synchronized on the devices in the FGSP cluster.
- FortiGate-6000 FGSP can use the HA1 and HA2 interfaces for session synchronization. FortiGate-7000 FGSP can use the 1-M1 and 1-M2 and 2-M1 and 2-M2 interfaces for session synchronization. For both FortiGate-6000 and FortiGate-7000 FGSP, using multiple interfaces is recommended for redundancy. To use these interfaces, you must give them IP addresses and optionally set up routing for them. Ideally the session synchronization interfaces

would be on the same network and that network would only be used for session synchronization traffic. However, you can configure routing to send session synchronization traffic between networks. NAT between session synchronization interfaces is not supported.
- Multiple VDOMs can be synchronized over the same session synchronization interface. You can also distribute synchronization traffic to multiple interfaces.
- FGSP doesn't support setting up IPv6 session filters using the `config session-sync-filter` option.
- FGSP doesn't synchronize ICMP sessions in DP to peer FortiGates when the default ICMP load balancing setting `to-master` is used. If you want to synchronize these sessions, ICMP load balancing should be set to either `src-ip`, `dst-ip`, or `src-dst-ip`. See ICMP load balancing on page 9 for more information.
- Asymmetric IPv6 SCTP traffic sessions are not supported. These sessions are dropped.
- Inter-cluster session synchronization, or FGSP between FGCP clusters, is not supported.
- FGSP IPsec tunnel synchronization is not supported.
- Fragmented packet synchronization is not supported.

FGSP session synchronization

The following session synchronization options apply to FGSP HA:

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

- Turning on session synchronization for TCP sessions by enabling `session-pickup` also turns on session synchronization for connectionless protocol sessions, such as ICMP and UDP, by enabling `session-pickup-connectionless`. You can choose to reduce processing overhead by not synchronizing connectionless sessions if you don't need to.
- The `session-pickup-expectation` and `session-pickup-nat` options only apply to FGSP HA. FGCP HA synchronizes NAT sessions when you enable `session-pickup`.
- The `session-pickup-delay` option applies to TCP sessions only and does not apply to connectionless and SCTP sessions.
- The `session-pickup-delay` option does not currently work for IPv6 TCP traffic. This known issue (553996) will be fixed in a future firmware version.
- The `session-pickup-delay` option should not be used in FGSP topologies where the traffic can take an asymmetric path (forward and reverse traffic going through different FortiGates).

Example FortiGate-6000 FGSP configuration

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

1. Configure the HA1 interface of the first FortiGate-6301F with an IP address on the 172.25.177.0/24 network:
   ```
   config system interface
      edit ha1
         set ip 172.25.177.10 255.255.255.0
      end
   ```
2. Configure the HA1 interface of the second FortiGate-6301F with an IP address on the 172.25.177.0/24 network:

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

3. On the first FortiGate-6301F, configure session synchronization for the root VDOM.

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

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

4. On the second FortiGate-6301F, configure session synchronization for the root VDOM.

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

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

Example FortiGate-7000 FGSP configuration

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

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

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

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

```
config system interface
   edit 1-M1
      set ip 172.25.177.40 255.255.255.0
   next
   edit 1-M2
      set ip 172.25.178.45 255.255.255.0
   end
```

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

```
config system cluster-sync
   edit 1
      set peervd mgmt-vdom
```

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

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

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

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

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

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

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

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for FortiGate-6000 and FortiGate-7000 v6.0.4 build 8405.

Default Security Fabric configuration

The FortiGate-6000 uses the Security Fabric for communication and synchronization between the management board and FPCs. The FortiGate-7000 uses the Security Fabric for communication and synchronization among FIMs and FPMs. Changing the default Security Fabric configuration could disrupt this communication and affect system performance.

Default Security Fabric configuration:

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

For the FortiGate-6000 and FortiGate-7000 to operate normally, you must not change the Security Fabric configuration.

Adding a flow rule to support DHCP relay

The FortiGate-6000 and FortGate-7000 default flow rules may not handle DHCP relay traffic correctly.

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

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

```
      set src-addr-ipv4 0.0.0.0 0.0.0.0
      set dst-addr-ipv4 0.0.0.0 0.0.0.0
      set protocol udp
      set src-l4port 68-68
      set dst-l4port 67-67
      set action forward
      set forward-slot master
      set priority 5
      set comment "dhcpv4 client to server"
   end
```

These flow rules handle traffic when the DHCP client sends requests to a DHCP server using port 68 and the DHCP server responds using port 67. However, if DHCP relay is involved, requests from the DHCP relay to the DHCP server and replies from the DHCP server to the DHCP relay both use port 67. If this DHCP relay traffic passes through the FortiGate-6000 or 7000 you must add a flow rule similar to the following to support port 67 DHCP traffic in both directions:

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

Limitations of installing FortiGate-6000 firmware from the BIOS after a reboot

Installing or upgrading FortiGate-6000 firmware from the BIOS installs firmware on and resets the configuration of the management board only. The FPCs will continue to operate with their current configuration and firmware build. The FortiGate-6000 system does not synchronize firmware upgrades performed from the BIOS.

See Installing FortiGate-6000 firmware from the BIOS after a reboot for detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

Limitations of installing FortiGate-7000 firmware from the BIOS after a reboot

Installing or upgrading FortiGate-7000 firmware from the BIOS installs firmware on and resets the configuration of the primary FIM only. The other FIM and the FPMs will continue to operate with their current configuration and firmware

build. The FortiGate-7000 system does not synchronize firmware upgrades performed from the BIOS.

See Installing firmware on individual FIMs and FPMs for detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

Installing firmware on an individual FortiGate-6000 FPC

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

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

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

   ```
   FPC6KFT018901327, Slave, uptime=615368.33, priority=19, slot_id=1:1, idx=1, flag=0x4, in_
   sync=1
   F6KF31T018900143, Master, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_
   sync=1
   FPC6KFT018901372, Slave, uptime=615319.63, priority=20, slot_id=1:2, idx=1, flag=0x4, in_
   sync=1
   F6KF31T018900143, Master, uptime=615425.84, priority=1, slot_id=1:0, idx=0, flag=0x10, in_
   sync=1
   FPC6KFT018901346, Slave, uptime=423.91, priority=21, slot_id=1:3, idx=1, flag=0x4, in_
   sync=1
   ```

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

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

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

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

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

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

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

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

5. Once the FPM is operating normally, log back in to the primary FIM CLI and enter the following command to reset the FPM to normal operation:

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

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

SD-WAN is not supported

FortiGate-6000 and FortiGate-7000 Version v6.0.4 does not support SD-WAN because of the following known issues:

- 524863, volume-based SD-WAN load balancing is not supported.
- 510522, when a link in an SD-WAN goes down and comes up, duplicate default routes are created on the management board.
- 510818, traffic from internal hosts is forwarded to destination servers even if SD-WAN health-checking determines that the server is down.
- 510389, SD-WAN usage is not updated on the management board GUI.
- 494019, SD-WAN monitor statistics are not updated on the management board GUI.
- 511091, SD-WAN load balancing rules based on packet loss, jitter, or latency do not work correctly.

IPsec VPN features that are not supported

FortiOS 6.0 for FortiGate-6000 and FortiGate-7000 does not support the following IPsec VPN features:

- Policy-based IPsec VPN.
- Policy routes for VPN traffic.
- Remote networks with 0- to 15-bit netmasks.
- IPv6 clear-text traffic (IPv6 over IPv4 or IPv6 over IPv6).
- FortiGate-7000 Load-balancing IPsec VPN tunnels to multiple FPMs. (FortiGate-6000 supports load balancing IPsec VPN tunnels to multiple FPCs, but with some limitations.)
- IPsec SA synchronization between HA peers.

Quarantine to disk not supported

The FortiGate-6000 platform, including the FortiGate-6301F and the FortiGate-6501F, and the FortiGate-7000 platform does not support quarantining files to the internal hard disks. Instead you must set the quarantine function to quarantine files to FortiAnalyzer.

Local out traffic is not sent to IPsec VPN interfaces

On most FortiGate platforms, an administrator can test an IPsec tunnel by opening the FortiGate CLI and pinging a remote host on the network at the other end of the IPsec VPN tunnel. This is not currently supported by the FortiGate-6000 and FortiGate-7000 platforms.

Special configuration required for SSL VPN

Using a FortiGate-6000 or a FortiGate-7000 as an SSL VPN server requires you to manually add an SSL VPN load balance flow rule to configure the FortiGate-6000 or FortiGate-7000 to send all SSL VPN sessions to the primary (master) FPC (FortiGate-6000) or the primary (master) FPM (FortiGate-7000). To match with the SSL VPN server traffic, the rule should include a destination port that matches the destination port of the SSL VPN server. A basic rule to allow SSL VPN traffic could be:

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

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

Adding the SSL VPN server IP address

You can add the IP address of the FortiGate-6000 or FortiGate-7000 interface that receives SSL VPN traffic to the SSL VPN flow rule to make sure that the flow rule only matches SSL VPN server settings. For example, if the IP address of the interface is 172.25.176.32 and the SSL VPN flow rule ID is 26:

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

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

If you change the SSL VPN server listening port

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

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

Management traffic limitations

FortiGate-6000 and FortiGate-7000 platforms support management traffic over out of band (OOB) management interfaces only:

- The FortiGate-6000 MGMT 1 to 3 interfaces on the FortiGate-6000.
- The FortiGate-7000 mgmt static LAG interface on the FortiGate-7000 FIMs. The mgmt LAG includes the MGMT 1 to 4 interfaces and this LAG configuration should not be changed.

Using data interfaces for management traffic is currently not supported. The following command is available to allow management traffic over data interfaces in a VDOM, but this command is currently not recommended as the feature is still under development.

```
config vdom
   edit <vdom-name>
      config system settings
         set motherboard-traffic-forwarding admin
   end
```

Managing individual FortiGate-6000 management boards and FPCs

The table below lists the special port numbers required to manage individual FortiGate-6000 FPCs.

If the system management IP address is 192.168.1.99, you can connect to the GUI of the first FPC using the system management IP address followed by the special port number: https://192.168.1.99:44301.

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

You can also use similar special port numbers to log into both management boards and individual FPCs in both FortiGate-6000s in an HA configuration. For example, if the management IP address is 192.168.1.99 you can browse to https://192.168.1.99:44323 to connect to the FPC in chassis 2 slot 3. The special port number (in this case 44323) is a combination of the service port, chassis ID, and slot number. For the components in chassis 1 the special port numbers are the same as those listed below (the chassis ID is 0). For the components in chassis 2 just add the chassis ID of 2 before the slot number.

From the CLI you can also use the `execute load-balance slot manage [<chassis>.]<slot>` command to log into the CLI of different components.

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

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

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

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

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

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

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

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

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

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

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

FortiGate-6000 special management port numbers

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8000	44300	2300	2200	16100
Slot 1 (FPC01)	8001	44301	2301	2201	16101
Slot 2 (FPC02)	8002	44302	2302	2202	16102
Slot 3 (FPC03)	8003	44303	2303	2203	16103
Slot 4 (FPC04)	8004	44304	2304	2204	16104
Slot 5 (FPC05)	8005	44305	2305	2205	16105

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 6 (FPC06)	8006	44306	2306	2206	16106
Slot 7 (FPC07)	8007	44307	2307	2207	16107
Slot 8 (FPC08)	8008	44308	2308	2208	16108
Slot 9 (FPC09)	8009	44309	2309	2209	16109
Slot 10 (FPC10)	8010	44310	2310	2210	16110

Managing individual FortiGate-7000 FIMs and FPMs

The following table lists the special port numbers required to manage individual FortiGate-7000 FIMs and FPMs.

From the FortiGate-7000 you can also use the `execute load-balance slot manage [<chassis>.]<slot>` command to log into individual FIMs and FPMs.

FortiGate-7000 special management port numbers

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

Example FortiGate-6000 switch configuration

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

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

This example shows how to configure a FortiGate-6000 to use different VLAN IDs for the HA1 and HA2 HA heartbeat interfaces and then how to configure two 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-6000s in the HA configuration, enter the following command to use different VLAN IDs for the HA1 and HA2 interfaces. The command sets the ha1 VLAN ID to 4091 and the ha2 VLAN ID to 4092:

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

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

```
get system ha status
...
HBDEV stats:
 F6KF51T018900026(updated 4 seconds ago):
  ha1: physical/10000full, up, rx-bytes/packets/dropped/errors=54995955/230020/0/0,
tx=63988049/225267/0/0, vlan-id=4091
  ha2: physical/10000full, up, rx-bytes/packets/dropped/errors=54995955/230020/0/0,
tx=63988021/225267/0/0, vlan-id=4092
 F6KF51T018900022(updated 3 seconds ago):
  ha1: physical/10000full, up, rx-bytes/packets/dropped/errors=61237440/230023/0/0,
tx=57746989/225271/0/0, vlan-id=4091
  ha2: physical/10000full, up, rx-bytes/packets/dropped/errors=61238907/230023/0/0,
tx=57746989/225271/0/0, vlan-id=4092
...
```

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

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

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

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

Example FortiGate-7000 switch configuration

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

This configuration is not required for FortiGate-7030E HA configurations if you have set up direct connections between the HA heartbeat interfaces.

This example shows how to configure a FortiGate-7000 to use different VLAN IDs for the M1 and M2 HA heartbeat interfaces and then how to configure two ports on a Cisco switch to allow HA heartbeat packets.

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

1. On both FortiGate-7000s in the HA configuration, enter the following command to use different VLAN IDs for the M1 and M2 interfaces. The command sets the M1 VLAN ID to 4086 and the M2 VLAN ID to 4087:

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

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

```
get system ha status
...
HBDEV stats:
 FG74E83E16000015(updated 1 seconds ago):
   1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=579602089/2290683/0/0,
tx=215982465/761929/0/0, vlan-id=4086
   2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=577890866/2285570/0/0,
tx=215966839/761871/0/0, vlan-id=4086
   1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=579601846/2290682/0/0,
tx=215982465/761929/0/0, vlan-id=4087
   2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=577890651/2285569/0/0,
tx=215966811/761871/0/0, vlan-id=4087
 FG74E83E16000016(updated 1 seconds ago):
   1-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=598602425/2290687/0/0,
tx=196974887/761899/0/0, vlan-id=4086
   2-M1: physical/10000full, up, rx-bytes/packets/dropped/errors=596895956/2285588/0/0,
tx=196965052/761864/0/0, vlan-id=4086
   1-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=598602154/2290686/0/0,
tx=196974915/761899/0/0, vlan-id=4087
   2-M2: physical/10000full, up, rx-bytes/packets/dropped/errors=596895685/2285587/0/0,
tx=196965080/761864/0/0, vlan-id=4087
...
```

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

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

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

```
interface <name>
switchport mode trunk
```

```
switchport trunk native vlan 777
switchport trunk allowed vlan 4087
```

Default FortiGate-6000 and FortiGate-7000 configuration for traffic that cannot be load balanced

The default `configure load-balance flow-rule` command contains the recommended default flow rules that control how the FortiGate-6000 or FortiGate-7000 handles traffic types that cannot be load balanced. The FortiGate-6000 and FortiGate-7000 have different settings for flow rules 21, 22, 23, and 24.

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

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

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

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

If you disable IP sec VPN load balancing by setting `ipsec-load-balance` to `disable`, the FortiGate-6000 or FortiGate-7000 automatically enables the IPsec VPN flow rules and sends all IPsec VPN traffic to the primary FPC or FPM.

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

Default FortiGate-6000 configuration for traffic that cannot be load balanced

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

```
        set src-l4port 0-0
        set dst-l4port 88-88
        set action forward
        set forward-slot master
        set priority 5
        set comment "kerberos dst"
    next
    edit 3
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 179-179
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp src"
    next
    edit 4
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 179-179
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp dst"
    next
    edit 5
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 520-520
        set dst-l4port 520-520
        set action forward
        set forward-slot master
        set priority 5
        set comment "rip"
    next
    edit 6
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 521-521
        set dst-l4port 521-521
        set action forward
        set forward-slot master
```

```
        set priority 5
        set comment "ripng"
    next
    edit 7
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 67-67
        set dst-l4port 68-68
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 server to client"
    next
    edit 8
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 68-68
        set dst-l4port 67-67
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 client to server"
    next
    edit 9
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 1723-1723
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp src"
    next
    edit 10
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1723-1723
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp dst"
```

```
next
edit 11
    set status enable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 0-0
    set dst-l4port 3784-3784
    set action forward
    set forward-slot master
    set priority 5
    set comment "bfd control"
next
edit 12
    set status enable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 0-0
    set dst-l4port 3785-3785
    set action forward
    set forward-slot master
    set priority 5
    set comment "bfd echo"
next
edit 13
    set status enable
    set vlan 0
    set ether-type ipv6
      set src-addr-ipv6 ::/0
    set dst-addr-ipv6 ::/0
    set protocol udp
    set src-l4port 547-547
    set dst-l4port 546-546
    set action forward
    set forward-slot master
    set priority 5
    set comment "dhcpv6 server to client"
next
edit 14
    set status enable
    set vlan 0
    set ether-type ipv6
    set src-addr-ipv6 ::/0
    set dst-addr-ipv6 ::/0
    set protocol udp
    set src-l4port 546-546
    set dst-l4port 547-547
    set action forward
    set forward-slot master
    set priority 5
    set comment "dhcpv6 client to server"
next
edit 15
    set status enable
    set vlan 0
```

```
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 224.0.0.0 240.0.0.0
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 multicast"
    next
    edit 16
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ff00::/8
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 multicast"
    next
    edit 17
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 2123-2123
        set action forward
        set forward-slot master
        set priority 5
        set comment "gtp-c to master blade"
    next
    edit 18
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike"
    next
    edit 19
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
```

```
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike-natt dst"
    next
    edit 20
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol esp
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 esp"
    next
    edit 21
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike"
    next
    edit 22
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike-natt dst"
    next
    edit 23
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol esp
        set action forward
        set forward-slot master
```

```
        set priority   5
        set comment "ipv4 esp"
    next
    edit 24
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1000-1000
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd http to master blade"
    next
    edit 25
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1003-1003
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd https to master blade"
    next
    edit 26
        set status enable
        set vlan 0
        set ether-type ip
        set protocol vrrp
        set action forward
        set forward-slot all
        set priority 6
        set comment "vrrp to all blades"
    next
end
```

Default FortiGate-7000 configuration for traffic that cannot be load balanced

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

```
next
edit 2
    set status disable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 0-0
    set dst-l4port 88-88
    set action forward
    set forward-slot master
    set priority 5
    set comment "kerberos dst"
next
edit 3
    set status enable
    set vlan 0
    set ether-type ip
    set protocol tcp
    set src-l4port 179-179
    set dst-l4port 0-0
    set tcp-flag any
    set action forward
    set forward-slot master
    set priority 5
    set comment "bgp src"
next
edit 4
    set status enable
    set vlan 0
    set ether-type ip
    set protocol tcp
    set src-l4port 0-0
    set dst-l4port 179-179
    set tcp-flag any
    set action forward
    set forward-slot master
    set priority 5
    set comment "bgp dst"
next
edit 5
    set status enable
    set vlan 0
    set ether-type ip
    set protocol udp
    set src-l4port 520-520
    set dst-l4port 520-520
    set action forward
    set forward-slot master
    set priority 5
    set comment "rip"
next
edit 6
    set status enable
    set vlan 0
    set ether-type ipv6
    set src-addr-ipv6 ::/0
```

```
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 521-521
        set dst-l4port 521-521
        set action forward
        set forward-slot master
        set priority 5
        set comment "ripng"
    next
    edit 7
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 67-67
        set dst-l4port 68-68
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 server to client"
    next
    edit 8
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 68-68
        set dst-l4port 67-67
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 client to server"
    next
    edit 9
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 1723-1723
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp src"
    next
    edit 10
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
```

```
        set dst-l4port 1723-1723
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp dst"
    next
    edit 11
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 3784-3784
        set action forward
        set forward-slot master
        set priority 5
        set comment "bfd control"
    next
    edit 12
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 3785-3785
        set action forward
        set forward-slot master
        set priority 5
        set comment "bfd echo"
    next
    edit 13
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 547-547
        set dst-l4port 546-546
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 server to client"
    next
    edit 14
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 546-546
        set dst-l4port 547-547
        set action forward
        set forward-slot master
```

```
        set priority 5
        set comment "dhcpv6 client to server"
    next
    edit 15
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 224.0.0.0 240.0.0.0
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 multicast"
    next
    edit 16
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ff00::/8
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 multicast"
    next
    edit 17
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 2123-2123
        set action forward
        set forward-slot master
        set priority 5
        set comment "gtp-c to master blade"
    next
    edit 18
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike"
    next
    edit 19
```

```
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike-natt dst"
    next
    edit 20
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol esp
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 esp"
    next
    edit 21
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike"
    next
    edit 22
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike-natt dst"
    next
    edit 23
        set status enable
        set vlan 0
```

```
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol esp
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 esp"
    next
    edit 24
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1000-1000
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd http to master blade"
    next
    edit 25
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1003-1003
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "authd https to master blade"
    next
    edit 26
        set status enable
        set vlan 0
        set ether-type ip
        set protocol vrrp
        set action forward
        set forward-slot all
        set priority 6
        set comment "vrrp to all blades"
    next
end
```

Upgrade information

This section provides upgrade information for upgrading your FortiGate-6000 or FortiGate-7000 to FortiOS v6.0.4 build 8405.

Upgrading a FortiGate-6000 or FortiGate-7000 HA configuration

Upgrading a FortiGate-6000 or FortiGate-7000 HA cluster with `uninterruptable-upgrade` enabled (called a graceful upgrade) to FortiOS v6.0.4 build 8405 is supported from the following builds:

- FortiOS v5.6.7 build 4214
- FortiOS v5.6.7 build 4261
- FortiOS v6.0.4 build 6145

Upgrading a FortiGate-6000 or FortiGate-7000 HA cluster with `uninterruptable-upgrade` enabled is not supported from FortiOS v6.0.4 build 8385 and FortiOS v5.6.7 build 4254.

If you disable `uninterruptible-upgrade`, the firmware upgrade occurs simultaneously across all hardware components and is supported from any build. However, you should still follow the correct recommended upgrade path as listed on https://support.fortinet.com under Upgrade path.

You can check the firmware version and build number from the System Information dashboard widget or from the CLI using the `get system status` command.

FortiGate-6000 upgrade information

FortiGate-6000 v6.0.4 build 8405 supports upgrading from FortiGate-6000 v5.6.7 build 4214 or 4261 or from v6.0.4 build 6145 to v6.0.4 build 8405.

For a FortiGate-6000 HA configuration, you can enable uninterruptible upgrade.

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

Enabling `uninterruptable-upgrade` allows you to upgrade the firmware of an operating FortGate-6000 HA configuration with only minimal traffic interruption. During the upgrade, the backup FortiGate-6000 upgrades first. Then a failover occurs and the newly upgraded FortiGate-6000 becomes the primary FortiGate-6000 and the firmware of the new backup FortiGate-6000 upgrades.

The management board and the FPCs in your FortiGate-6000 system run the same firmware image. You upgrade the firmware using the management board GUI or CLI just as you would any FortiGate product. During the upgrade process, the firmware running on the management board and all of the FPCs upgrades in one step. Firmware upgrades

should be done during a quiet time because traffic will be briefly interrupted during the upgrade process. The entire firmware upgrade takes a few minutes, depending on the number of FPCs in your FortiGate-6000 system. Some firmware upgrades may take longer depending on factors, such as the size of the configuration and whether an upgrade of the DP processor is included.

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

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

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

FortiGate-7000 upgrade information

FortiGate-7000 6.0.4 build 8405 supports upgrading from FortiGate-7000 v5.6.7 build 4214 or 4261 or from v6.0.4 build 6145 to 6.0.4 build 8405.

For a FortiGate-7000 HA configuration, you can enable uninterruptible upgrade.

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

Enabling `uninterruptable-upgrade` allows you to upgrade the firmware of an operating FortGate-7000 HA configuration with only minimal traffic interruption. During the upgrade, the backup FortiGate-7000 upgrades first. Then a failover occurs and the newly upgraded FortiGate-7000 becomes the primary FortiGate-7000 and the firmware of the new backup FortiGate-7000 upgrades.

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

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

- Review the latest release notes for the firmware version that you are upgrading to.
- Verify the recommended upgrade path as documented in the release notes.
- Back up your FortiGate-7000 configuration.

Fortinet recommends that you review the services provided by your FortiGate-7000 before a firmware upgrade and then again after the upgrade to make sure the services continues to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade, and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

Product integration and support

See the Product integration and support section of the FortiOS 6.0.4 release notes for product integration and support information for FortiGate-6000 and FortiGate-7000 v6.0.4.

Also please note the following exceptions for FortiGate-6000 and FortiGate-7000 v6.0.4 build 8405:

Minimum recommended FortiManager firmware version : 6.0.5 and 6.2.1.

Minimum recommended FortiAnalyzer firmware version : 6.0.5 and 6.2.1.

FortiGate-6000 v6.0.4 special features and limitations

FortiGate-6000 v6.0.4 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-6000 v6.0.4 section of the FortiGate-6000 handbook.

FortiGate-7000 v6.0.4 special features and limitations

FortiGate-7000 v6.0.4 has specific behaviors that may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000 v6.0.4 section of the FortiGate-7000 handbook.

Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 6.0.4 are available from the FortiOS 6.0.4 Maximum Values Table.

Resolved issues for build 8405

The following issues have been fixed in FortiGate-6000 and FortiGate-7000 FortiOS v6.0.4 build 8405. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
574564	Resolved an issue that caused synchronization errors and disrupted operations after upgrading an HA cluster with `uninterruptable-upgrade` enabled.

Resolved issues for build 8385

The following issues have been fixed in FortiGate-6000 and FortiGate-7000 FortiOS v6.0.4 build 8385. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
555410	Resolved an issue that prevented synchronizing application control signatures between the FortiGate-6000 management board and the FPCs or between the FortiGate-7000 primary FIM and the other FIM and FPMs.
538904	Resolved an issue that sometimes prevented SSLVPN clients from receiving SSL tunnel IP addresses.
540328 542706	Resolved an issue with SSL VPN web mode that sometimes blocked access to some internal resources.
567434	Resolved an issue that sometimes caused individual FortiGate-6000 FPCs or FortiGate-7000 FPMs to fail to resolve domain names after a system restart because DNS server information was not initialized correctly.

Common vulnerabilities and exposures

Visit https://fortiguard.com/psirt for more information.

Vulnerability
FortiGate-6000F and 7000E v6.0.4,build 8385, (GA) is no longer vulnerable to https://fortiguard.com/psirt/FG-IR-19-144.

Bug ID	CVE references
529745	FortiOS 6.0.4 for FortiGate-6000 and 7000 series is no longer vulnerable to the following CVE Reference: • CVE-2018-13382 (see: https://fortiguard.com/psirt/FG-IR-18-389)
529353	FortiOS 6.0.4 for FortiGate-6000 and 7000 series is no longer vulnerable to the following CVE Reference: • CVE-2018-13380 (see: https://fortiguard.com/psirt/FG-IR-18-383)
452730	FortiOS 6.0.4 for FortiGate-6000 and 7000 series is no longer vulnerable to the following CVE Reference: • CVE-2017-14186 (see: https://fortiguard.com/psirt/FG-IR-17-242)
539553	FortiOS 6.0.4 for FortiGate-6000 and 7000 series is no longer vulnerable to the following CVE References: • CVE-2019-5586 and CVE-2019-5588 (see: https://fortiguard.com/psirt/FG-IR-19-034)

Bug ID	CVE references
529719	FortiOS 6.0.4 for FortiGate-6000 and 7000 series is no longer vulnerable to the following CVE Reference: • CVE-2018-13383 (see: https://fortiguard.com/psirt/FG-IR-18-388)
529377	FortiOS 6.0.4 for FortiGate-6000 and 7000 series is no longer vulnerable to the following CVE Reference: • CVE-2018-13379 (see: https://fortiguard.com/psirt/FG-IR-18-384)

Resolved issues for build 6145

The following issues have been fixed in FortiGate-6000 and FortiGate-7000 FortiOS v6.0.4 build 6145. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
525063	Incorrectly configuring HA with only one heartbeat interface now displays an error message.
525612	Resolved an issue that prevented IPv6 traceroute and ping from working when logged into an FIM console.
525619	Ping and traceroute sessions initiated from an FIM or FPM CLI can now be stopped.
526030	HA nodes no longer failover when processes were restarted after an antivirus database update.
526252	Resolved an issue that caused the `updated` process to use extra memory.
526387	The `source-ip` is now available when configuring per-vdom log settings.
526393	The per-vdom log `override-setting` option now works as expected.
526396	The `source` option of the `execute traceroute-option` command is once again available when logged into the CLI of an FIM.
527206	The `execute ping-option` command now works as expected from an FIM CLI.
526531	Resolved an issue that displayed Network is unreachable messages in ADVPN BFD debug messages.
543009	Resolved an issue caused by the `slbd` process starting out of sequence.
543382	NAT session synchronization is now enabled correctly when `session-pickup` is enabled for FGCP HA.
543967	The `diagnose load-balance switch stats clear <eid>` command no longer clears all switch stats.
545686	The `diagnose load-balance switch stats clear` command now successfully clears all switch stats.
544160	Resolved an issue that caused Signal 11 crashes related to long VDOM names.
544748	In an HA configuration, the backup chassis can now connect to the configured NTP server if the NTP configuration includes a `source-ip` setting.
545112 542562	Resolved multiple issues that sometimes prevented the configuration from being restored correctly from a backup file.
545125	Resolved an issue that blocked connections to the mgmt interface.
545601	Resolved a configuration synchronization issues with cross-FIM LAG DP ingress-trunk-mapping.
545670	Resolved an RSYNC loop that generated extra sessions.
527369	Fixed errors that occurred when generating the TAC report using the `execute tac report`

Bug ID	Description
	command.
527549	Improvements to FortiGate-7000 licensing.
527709	Resolved issues that caused problems after master FPC failover.
527995	The `diagnose sys confsync diffcsum` command now displays information.
528704	Resolved a zombie kernel thread issue.
528760	Resolved an issue that prevented FortiToken activations.
529497	Web-proxy traffic logs now include the `utmref` field as expected.
531260	The `diagnose sys session6 filter` command can now include a policy ID.
532390	Resolved an issue that sometimes displayed error messages similar to cwEncryptKeyRstHandler failed to generate vdom xxx key.
533051	The FortiGate-7000 System Information dashboard widget no longer shows the primary FIM serial number instead of the FortiGate-7000 chassis serial number.
533124	Resolved an HA issue that incorrectly synchronized Cross-FIM LAG DP Peer-SYNC sessions between chassis.
533453	Resolved an issue that incorrectly caused an HA failover after restarting an FPM on the primary chassis when `board-failover-tolerance` is set to 1.
533949	Diagnose command options and output that only apply to FortiGate-7000 HA have been removed from FortiGate-6000.
534766	Resolved an issue that caused LAG ports to drop PDQ_OSW_EHP sessions.
535397	The Antivirus quarantine configuration no longer defaults to quarantine to disk.
535457	Resolved an issue caused by setting some interface speeds to 1000auto.
535549	Resolved an issue that could interrupt communication between chassis in an HA configuration after a firmware upgrade.
537732	Resolved an issue that caused the system time to be incorrect after being set manually from the CLI.
538335	After restoring the configuration of a VDOM on the management board or primary FIM, the restored VDOM configuration is now successfully synchronized to all FPCs, or FIMs and FPMs.
539876	Resolved an issue that incorrectly caused the diagnose debug flow filter command output to be broadcast.
540123	The Policy & Objects and Security Profiles pages have been removed from mgmt-vdom GUI.
540256	Resolved an issue that caused policy counters to remain zero on the FIM GUI firewall policy page.
540668	Resole several issues that caused errors when restoring the configuration from a backup file.
540848	Resolved an issue that caused the `diagnose test application hatalk` command to display incorrect information.

Bug ID	Description
541049	Resolved an issue related to enabling scanning outgoing connections to botnet sites that caused sessions to reset.
541670	The `diagnose hardware deviceinfo psu` command no longer returns error messages.
547220	Resolved an issue that caused the DP processor session count to incorrectly increase because of fragmented ICMPv4 traffic.
548497	Resolved an issue that displayed ha_shm_mutex_enter error messages when enabling active-passive HA.
548969	For the FortiGate-6300, 6500 and all 7000 platforms, the crash log size has been increased to 800k.
550134	Resolved an issue that caused the `hatalk` process to use excessive amounts of CPU time when enabling or disabling an individual FPC or FPM.
550687	Resolved an issue that sometimes caused a disabled FPM to become the primary FPM.

Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 FortiOS v6.0.4 build 8405. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
523521	The Security Fabric widget does not indicate which FPC or FPM is the primary (master).
539081	SSL VPN can't listen on LACP LAG interfaces.
550313	Virtual servers with SSL offloading generate TLS errors and do not forward traffic.
495029	Tunnel mode SSL VPN is not working when using `ip-range` as the tunnel address pool.
513701	Local out traffic from the management board (for example a ping request) is not send from the management board to an IPsec tunnel.
513928	IPsec tunnels using Secondary IPs do not start up.
506732	On the FortiGate-6301F and 6501F, `config antivirus quarantine` does not allow saving quarantine files to disk.
530765	The `miglogd` process sometimes crashes due to a segmentation fault, recording a signal 11 error message
548305	During some testing involving UDP traffic, log messages are not recorded for dropped packets..
538851	In some configurations, outgoing packets have incorrect VLAN tags.
546813	Traffic interface status is sometimes not correctly synchronized from FIMs to FPMs.
541234	The FortiGate-7060E only shows the status of power supplies in PSU slots 1 to 4.
548923	CLI commands can show incorrect transceiver stats.
547481	EMAC VLANs do not work as expected.
549983 474410	Cannot establish management connections to FortiGate-6000 or 7000 traffic interfaces.
491439	The HA `route-ttl` option is not available.
475169	The `updated` process crashes when performing antivirus and IPS updates.
459424	The statistics appearing on the VDOM GUI page are not accurate.
551239	For a FortiGate-6000 or 7000 HA cluster with uninterruptable upgrade enabled, some sessions that should be synchronized after a firmware upgrade are not.
550664	Interface Bandwidth dashboard widgets sometimes show excessive bandwidth usage.
510818	Traffic from internal hosts to an SD-WAN health-check server is forwarded even when all WAN links are down.
510522	When one of the links in an SD-WAN interface goes down and comes up, duplicate default routes

Bug ID	Description
	appear on the management board Routing Monitor.
511091	SD-WAN load balancing rules based on packet-loss, jitter, or latency do not work correctly.
549127	Fragmented traffic does not pass through IPsec tunnels.
514361	Outgoing IPsec VPN clear-txt traffic is sometimes load-balanced to the wrong FPCs or FPMs.
549166	BGP SNMP queries to the management IP address do not work unless connect to an individual FPC or FPM using the special management port numbers.
549806	The configuration of the dashboard may be lost after upgrading from FortiOS 5.6.6 to 6.0.4.
549567	On FortiGate-7000 platforms, the `diagnose hardware deviceinfo psu` command does not display any information.
550945	Upgrading the firmware from a USB key may flag the upgrade as a firmware downgrade.