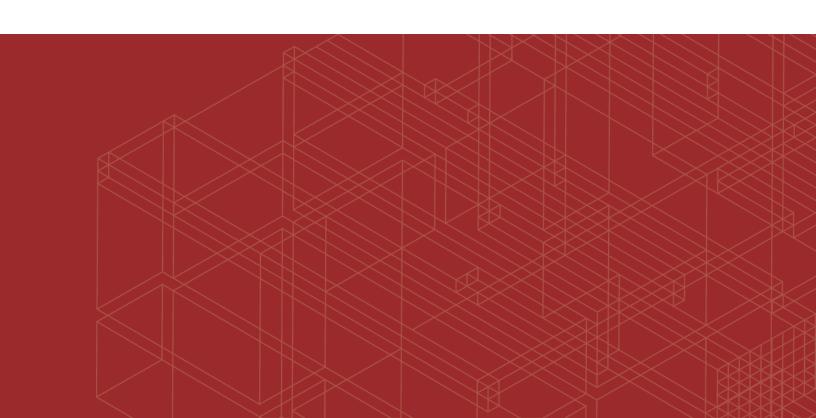# FortiGate-6000 and FortiGate-7000 - Release Notes

Version 5.6.11 Build 4279

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

F⊟RTINET®

TABLE OF CONTENTS

Change log

Date	Change description
October 28, 2019	Misc fixes.
October 4, 2019	Misc fixes.
October 3, 2019	Initial version.

Introduction

This document provides the following information for FortiGate-6000 and FortiGate-7000 5.6.11 Build 4279:

- Supported models
- What's new in FortiGate-6000 and FortiGate-7000 5.6.11 Build 4279
- Special notices
- Upgrade information
- Product integration and support
- Resolved issues
- Known issues

Supported models

FortiGate-6000 5.6.11 Build 4279 supports the following models:

- FortiGate-6300F
- FortiGate-6301F
- FortiGate-6500F
- FortiGate-6501F
- FortiGate-7030E
- FortiGate-7040E
- FortiGate-7060E

What's new in FortiGate-6000 and FortiGate-7000 5.6.11 Build 4279

FortiGate-6000 and FortiGate-7000 5.6.11 Build 4279 includes the bug fixes described in Resolved issues on page 33.

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 5.6.11 Build 4279.

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 at https://support.fortinet.com.

    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 at https://support.fortinet.com.

    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 5.6.11 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 5.6 for FortiGate-6000 and FortiGate-7000 does not support the following IPsec VPN features:

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

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 443-443
      set forward-slot master
      set comment "ssl vpn server to primary worker"
   next
   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 FPC. 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 FPC.

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. This example also sets the source interface to port12, which is the SSL VPN server interface, 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 10443-10443
      set forward-slot master
      set comment "ssl vpn server to primary worker"
   end
```

Adding the SSL VPN server IP address

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

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

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
```

Example FortiGate-6000 HA heartbeat 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-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 HA heartbeat 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-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 7000 handles traffic types that cannot be load balanced. 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. FortiGate-6000 and 7000 for FortiOS 6.0.6 have the same default flow rules.

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.

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.

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

```
config load-balance flow-rule
    edit 1
        set status disable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 88-88
        set dst-l4port 0-0
        set action forward
        set forward-slot master
        set priority 5
        set comment "kerberos src"
    next
    edit 2
        set status disable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 88-88
        set action forward
        set forward-slot master
        set priority 5
        set comment "kerberos dst"
    next
    edit 3
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 179-179
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp src"
    next
    edit 4
        set status enable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 179-179
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "bgp dst"
    next
    edit 5
```

```
            set status enable
            set vlan 0
            set ether-type ip
            set protocol udp
            set src-l4port 520-520
            set dst-l4port 520-520
            set action forward
            set forward-slot master
            set priority 5
            set comment "rip"
        next
        edit 6
            set status enable
            set vlan 0
            set ether-type ipv6
            set src-addr-ipv6 ::/0
            set dst-addr-ipv6 ::/0
            set protocol udp
            set src-l4port 521-521
            set dst-l4port 521-521
            set action forward
            set forward-slot master
            set priority 5
            set comment "ripng"
        next
        edit 7
            set status enable
            set vlan 0
            set ether-type ipv4
            set src-addr-ipv4 0.0.0.0 0.0.0.0
            set dst-addr-ipv4 0.0.0.0 0.0.0.0
            set protocol udp
            set src-l4port 67-67
            set dst-l4port 68-68
            set action forward
            set forward-slot master
            set priority 5
            set comment "dhcpv4 server to client"
        next
        edit 8
            set status enable
            set vlan 0
            set ether-type ipv4
            set src-addr-ipv4 0.0.0.0 0.0.0.0
            set dst-addr-ipv4 0.0.0.0 0.0.0.0
            set protocol udp
            set src-l4port 68-68
            set dst-l4port 67-67
            set action forward
            set forward-slot master
            set priority 5
            set comment "dhcpv4 client to server"
        next
        edit 9
            set status disable
            set vlan 0
```

```
            set ether-type ip
            set protocol tcp
            set src-l4port 1723-1723
            set dst-l4port 0-0
            set tcp-flag any
            set action forward
            set forward-slot master
            set priority 5
            set comment "pptp src"
        next
        edit 10
            set status disable
            set vlan 0
            set ether-type ip
            set protocol tcp
            set src-l4port 0-0
            set dst-l4port 1723-1723
            set tcp-flag any
            set action forward
            set forward-slot master
            set priority 5
            set comment "pptp dst"
        next
        edit 11
            set status enable
            set vlan 0
            set ether-type ip
            set protocol udp
            set src-l4port 0-0
            set dst-l4port 3784-3784
            set action forward
            set forward-slot master
            set priority 5
            set comment "bfd control"
        next
        edit 12
            set status enable
            set vlan 0
            set ether-type ip
            set protocol udp
            set src-l4port 0-0
            set dst-l4port 3785-3785
            set action forward
            set forward-slot master
            set priority 5
            set comment "bfd echo"
        next
        edit 13
            set status enable
            set vlan 0
            set ether-type ipv6
            set src-addr-ipv6 ::/0
            set dst-addr-ipv6 ::/0
            set protocol udp
            set src-l4port 547-547
            set dst-l4port 546-546
```

```
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 server to client"
    next
    edit 14
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 546-546
        set dst-l4port 547-547
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 client to server"
    next
    edit 15
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 224.0.0.0 240.0.0.0
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 multicast"
    next
    edit 16
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ff00::/8
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 multicast"
    next
    edit 17
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 2123-2123
        set action forward
        set forward-slot master
        set priority 5
        set comment "gtp-c to master blade"
```

```
            next
            edit 18
                set status enable
                set vlan 0
                set ether-type ipv6
                set src-addr-ipv6 ::/0
                set dst-addr-ipv6 ::/0
                set protocol udp
                set src-l4port 0-0
                set dst-l4port 500-500
                set action forward
                set forward-slot master
                set priority 5
                set comment "ipv6 ike"
            next
            edit 19
                set status enable
                set vlan 0
                set ether-type ipv6
                set src-addr-ipv6 ::/0
                set dst-addr-ipv6 ::/0
                set protocol udp
                set src-l4port 0-0
                set dst-l4port 4500-4500
                set action forward
                set forward-slot master
                set priority 5
                set comment "ipv6 ike-natt dst"
            next
            edit 20
                set status enable
                set vlan 0
                set ether-type ipv6
                set src-addr-ipv6 ::/0
                set dst-addr-ipv6 ::/0
                set protocol esp
                set action forward
                set forward-slot master
                set priority 5
                set comment "ipv6 esp"
            next
            edit 21
                set status disable
                set vlan 0
                set ether-type ipv4
                set src-addr-ipv4 0.0.0.0 0.0.0.0
                set dst-addr-ipv4 0.0.0.0 0.0.0.0
                set protocol udp
                set src-l4port 0-0
                set dst-l4port 500-500
                set action forward
                set forward-slot master
                set priority 5
                set comment "ipv4 ike"
            next
            edit 22
```

```
            set status disable
            set vlan 0
            set ether-type ipv4
            set src-addr-ipv4 0.0.0.0 0.0.0.0
            set dst-addr-ipv4 0.0.0.0 0.0.0.0
            set protocol udp
            set src-l4port 0-0
            set dst-l4port 4500-4500
            set action forward
            set forward-slot master
            set priority 5
            set comment "ipv4 ike-natt dst"
        next
        edit 23
            set status disable
            set vlan 0
            set ether-type ipv4
            set src-addr-ipv4 0.0.0.0 0.0.0.0
            set dst-addr-ipv4 0.0.0.0 0.0.0.0
            set protocol esp
            set action forward
            set forward-slot master
            set priority 5
            set comment "ipv4 esp"
        next
        edit 24
            set status enable
            set vlan 0
            set ether-type ip
            set protocol tcp
            set src-l4port 0-0
            set dst-l4port 1000-1000
            set tcp-flag any
            set action forward
            set forward-slot master
            set priority 5
            set comment "authd http to master blade"
        next
        edit 25
            set status enable
            set vlan 0
            set ether-type ip
            set protocol tcp
            set src-l4port 0-0
            set dst-l4port 1003-1003
            set tcp-flag any
            set action forward
            set forward-slot master
            set priority 5
            set comment "authd https to master blade"
        next
        edit 26
            set status enable
            set vlan 0
            set ether-type ip
            set protocol vrrp
```

```
            set action forward
            set forward-slot all
            set priority 6
            set comment "vrrp to all blades"
        next
    end
```

Managing individual FortiGate-6000 management boards and FPCs

You can manage individual FPCs using special management port numbers, FPC consoles, or the `execute load-balance slot manage` command. You can also use the `execute ha manage` command to log in to the other FortiGate-6000 in an HA configuration.

Special management port numbers

You may want to connect to individual FPCs 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 FPCs (or the management board) using the MGMT1 interface IP address with a special port number.

> You can use the `config load-balance setting slbc-mgmt-intf` command to change the management interface used. The default is `mgmt1` and it can be changed to `mgmt2`, or `mgmt3`.
>
> To enable using the special management port numbers to connect to individual FPCs, set `slbc-mgmt-intf` to an interface that is connected to a network, has a valid IP address, and has management or administrative access enabled. To block access to the special management port numbers you can set `slbc-mgmt-intf` to an interface that is not connected to a network, does not have a valid IP address, or has management or administrative access disabled.

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

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

The special port number (in this case, 44301) is a combination of the service port (for HTTPS, the service port is 443) and the FPC slot number (in this example, 01).

You can view the special HTTPS management port number for and log in to the GUI of an FPC from the Security Fabric dashboard widget.

The following table lists the special ports you can use to connect to individual FPCs or the management board using common management protocols. The FortiGate-6300F and 6301F have 7 slots (0 to 6) and the FortiGate-6500F and 6501F have 11 slots (0 to 10). Slot 0 is the management board (MBD) slot. Slots 1 to 10 are FPC slots.

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

FortiGate-6000 special management port numbers

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

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

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

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

HA mode special management port numbers

In an HA configuration consisting of two FortiGate-6000s in an HA cluster, you can connect to individual FPCs or to the management board in chassis 1 (chassis ID = 1) using the same special port numbers as for a standalone FortiGate-6000.

You use different special port numbers to connect to individual FPCs or the management board in the FortiGate-6000 with chassis ID 2 (chassis ID = 2).

FortiGate-6000 special management port numbers (chassis ID = 2)

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 0, (MBD)	8020	44320	2320	2220	16120
Slot 1 (FPC01)	8021	44321	2321	2221	16121
Slot 2 (FPC02)	8022	44322	2322	2222	16122

Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 3 (FPC03)	8023	44323	2323	2223	16123
Slot 4 (FPC04)	8024	44324	2324	2224	16124
Slot 5 (FPC05)	8025	44325	2325	2225	16125
Slot 6 (FPC06)	8026	44326	2326	2226	16126
Slot 7 (FPC07)	8027	44327	2327	2227	16127
Slot 8 (FPC08)	8028	44328	2328	2228	16128
Slot 9 (FPC09)	8029	44329	2329	2229	16129
Slot 10 (FPC10)	8030	44330	2330	2230	16130

Connecting to individual FPC consoles

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

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

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

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

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

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

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

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

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

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

Connecting to individual FPC CLIs

From the management board CLI you can use the following command to log into the CLI of individual FPCs:

```
execute load-balance slot manage <slot-number>
```

Where:

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

When connected to the CLI of a FPC, you can view information about the status or configuration of the FPC, restart the FPC, or perform other operations. You should not change the configuration of individual FPCs because this can cause configuration synchronization errors.

Performing other operations on individual FPCs

You can use the following commands to restart, power off, power on, or perform an NMI reset on individual FPCs while logged into the management board CLI:

```
execute load-balance slot {nmi-reset | power-off | power on | reboot} <slots>
```

Where `<slots>` can be one or more slot numbers or slot number ranges separated by commas. Do not include spaces.

For example, to shut down the FPCs in slots 2, and 4 to 6 enter:

```
execute load-balance slot power-off 2,4-6
```

Managing individual FortiGate-7000 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-7000 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-7000 using the mgmt interface IP address with a special port number.

> 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.

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

`https://192.168.1.99:44303`

The special port number (in this case 44303) is a combination of the service port (for HTTPS, the service port is 443) and the 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 Security Fabric dashboard widget.

The following table lists the special port numbers to use to connect to each FortiGate-7000 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.

FortiGate-7000 special management port numbers

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

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

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

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

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

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-7000 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	8005	44303	2303	2203	16103
Ch1 slot 1	FIM01	8003	44301	2301	2201	16101
Ch1 slot 2	FIM02	8002	44302	2302	2202	16102
Ch1 slot 4	FPM04	8004	44304	2304	2204	16104
Ch1 slot 6	FPM06	8006	44306	2306	2206	16106
Ch2 slot 5	FPM05	8005	44325	2325	2225	16125
Ch2 slot 3	FPM03	8005	44323	2323	2223	16123
Ch2 slot 1	FIM01	8003	44321	2321	2221	16121
Ch2 slot 2	FIM02	8002	44322	2322	2222	16122
Ch2 slot 4	FPM04	8004	44324	2324	2224	16124
Ch2 slot 6	FPM06	8006	44326	2326	2226	16126

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.

Upgrade information

This section provides upgrade information for upgrading your FortiGate-6000 or 7000 to FortiOS 5.6.11 Build 4279.

FortiGate-6000 upgrade information

FortiGate-6000 for FortiOS 5.6.11 Build 4279 supports upgrading from FortiGate-6000 for FortiOS 5.6.7 build 4261.

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 DP3 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 5.6.11 Build 4279 supports upgrading from FortiGate-7000 for FortiOS 5.6.7 build 4261.

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 5.6.11 release notes for product integration and support information for FortiGate-6000 and 7000 for FortiOS 5.6.11 Build 4279.

Also please note the following exceptions for FortiGate-6000 and 7000 for FortiOS 5.6.11 Build 4279:

- FortiGate-6000: FortiManager or FortiAnalyzer 6.0.7 or 6.2.3.
- FortiGate-7000: FortiManager or FortiAnalyzer 6.0.7 or 6.2.3.

FortiGate-6000 for FortiOS 5.6.11 special features and limitations

FortiGate-6000 for FortiOS 5.6.11 has specific behaviors that may differ from FortiOS features. For more information, see the "Special features and limitations for FortiGate-6000 v5.6.11" section of the most recent version of the FortiGate-6000 handbook for FortiOS 5.6.11: FortiGate-6000 for FortiOS 5.6.11 special features and limitations.

FortiGate-7000 for FortiOS 5.6.11 special features and limitations

FortiGate-7000 for FortiOS 5.6.11 has specific behaviors that may differ from FortiOS features. For more information, see the "Special features and limitations for FortiGate-7000 v5.6.11" section of the most recent version of the FortiGate-7000 handbook for FortiOS 5.6.11: FortiGate-7000 for FortiOS 5.6.11 special features and limitations.

Maximum values

Maximum values for FortiGate-6000 and 7000 for FortiOS 5.6.11 are available from the FortiOS 5.6.11 Maximum Values Table.

Resolved issues

The following issues have been fixed in FortiGate-6000 and 7000 FortiOS 5.6.11 Build 4279. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
538269	Resolved an issue when testing connectivity to an LDAP server from the GUI.
563912	Trunk IDs are now successfully synchronized after a graceful HA upgrade.
566108	Log VDOM names are now successfully synchronized after a system reboot.
572527	The `confsynchbd` process can now be successfully restarted.
580531	Resolved an issue that caused the `confsyncd` process to crash.
580709	Resolved an issue that caused to `hatalk` process to crash during a graceful HA firmware upgrade.
582337	Resolved an issue that caused the `foauthd` process to crash.
582542	Resolved an issue that caused error message to be displayed on the console during a graceful HA firmware upgrade.
582646	Resolved an issue that made it seem like a cluster would not be able to synchronize after resetting the backup FortiGate-6000 or 7000 to factory defaults.
583142	Resolved an issue that could prevent a graceful HA firmware upgrade from completing.
583805	Resolved an issue that could prevent the `dnsproxy` process from being able to connect to the management VDOM (mgmt-vdom).
584604	Resolved av configuration synchronization issue that occurred when changing the configuration of a firewall VIP.
524863	The SD-WAN `measured-volume-based` load balancing option has been removed because it is not supported by FortiGate-6000 and 7000 Session-Aware Load Balancing Clustering (SLBC).
548969	The crash log file size has been increased to 8k lines for FortiGate-7000 platforms and for the FortiGate-6300 and 6500.
582351	Resolved an issue that caused the `miglogd` process running on FPMs to crash.

Known issues

The following issues have been identified in FortiGate-6000 and 7000 5.6.11 Build 4279. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
459424	Statistics on the **System > VDOM** GUI page may be incorrect.
474410	In-band management through traffic interfaces is not supported for FortiOS 5.6.11.
537861	An FPM of a FortiGate-7000 in an HA cluster may become unresponsive and require a manual restart of the FPM to restore service.
549983	FortiManager in-band management connections to the IP address of a VDOM link interface are not supported.
561722	Firewall policies designed to identify traffic from known devices may not be able to detect traffic from the known devices.
562773	In some cases and more often in an FGCP HA cluster, FortiGuard rating services may not be synchronized to all FPCs or FPMs.
570796	Scheduled FortiGuard updates of a HA cluster may cause management heartbeat loss resulting in an HA failover.
575568	Transparent mode HA may not respond as expected if a monitored interface goes down but then comes back up quickly. In this situation gratuitous ARP packets may fail to update the mac addresses on attached switches.
575916	During a graceful upgrade of a FortiGate-6000 HA cluster, the backup FortiGate-6000 may become the primary before all of the FPCs in the new primary FortiGate-6000 are synchronized.
578485	During a graceful upgrade of a FortiGate-7000 HA cluster, the backup FortiGate-7000 may become the primary before all of the FPMs in the new primary FortiGate-7000 are running the new firmware image.
579284	A segmentation fault (signal 11) may cause version 3.543 of the IPS engine to crash.
579836	Adding and removing multiple VLAN interfaces may cause error messages to appear on the CLI and can result in the CLI and GUI becoming unresponsive. A system restart may be required to access the system.
583124	Incorrect usage information may be sent to a RADIUS server. Usage information can include the amount of data downloaded by a user or the amount of time that a user is connected.
584078	Server load balancing real server status may not be synchronized to all FPCs or FPMs.
584127	In some cases, changes to active firewall policies may not be synchronized to all FPCs or FPMs.
584420	Because of synchronization issues between FPCs or FPMs, a captive portal configuration may block user access after the user has successfully authenticated.
584800	The `confsyncd` process may crash when adding or deleting multiple VDOMs.
585239	Traffic logs may show unexpected results because outgoing short-lived UDP sessions may be directed to the wrong FPC or FPM.