FORTINET

FortiGate-6000 and FortiGate-7000 Release Notes

VERSION v5.6.7 Build 4261

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdoc@fortinet.com

August 27, 2019

FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261 Release Notes

01-567-576435-20190827

TABLE OF CONTENTS

Change log **5**
Introduction **6**
Supported models 6
What's new in FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261 6
Special notices **7**
Default security fabric configuration 7
Adding a flow rule to support DHCP relay 7
Limitations of installing FortiGate-6000 firmware from the BIOS after a reboot 8
Limitations of installing FortiGate-7000 firmware from the BIOS after a reboot 8
SD-WAN is not supported 9
IPsec VPN features that are not supported 9
Quarantine to disk not supported 9
Local out traffic is not sent to IPsec VPN interfaces 9
Special configuration required for SSL VPN 10
Adding the SSL VPN server IP address 10
If you change the SSL VPN server listening port 10
Management traffic limitations 11
Managing individual FortiGate-6000 management boards and FPCs 11
Managing individual FortiGate-7000 FIMs and FPMs 13
Default FortiGate-6000 and FortiGate-7000 configuration for traffic that cannot be load balanced 13
Upgrade information **18**
Upgrading a FortiGate-6000 or FortiGate-7000 HA configuration 18
Possible heartbeat communication issue when upgrading an HA cluster 18
Verifying the status of an HA configuration after a firmware upgrade 19
Example FortiGate-6000 switch configuration 19
Example FortiGate-7000 switch configuration 20
FortiGate-6000 upgrade information 21
FortiGate-7000 upgrade information 22
Product integration and support **24**
FortiGate-6000 v5.6.7 special features and limitations 24
FortiGate-7000 v5.6.7 special features and limitations 24
Maximum values 24
Resolved issues for build 4261 ..... **25**

Resolved issues for build 4254 ..... **26**
Common vulnerabilities and exposures 27
Resolved issues for build 4214 ..... **28**
Known issues **31**

Change log

Date	Change description
August 27, 2019	Added more information to Common vulnerabilities and exposures on page 27.
August 15, 2019	Updated for build 4261, a new bug fix release of FortiGate-6000 and FortiGate-7000 for FortiOS 5.6.7. New sections: Upgrading a FortiGate-6000 or FortiGate-7000 HA configuration on page 18 and Resolved issues for build 4261 on page 25.
July 26, 2019	Updated for build 4254, a new bug fix release of FortiGate-6000 and FortiGate-7000 for FortiOS 5.6.7. New section: Resolved issues for build 4254 on page 26.
July 5, 2019	New section: Adding a flow rule to support DHCP relay on page 7.
June 21, 2019	New sections: Default security fabric configuration on page 7 and Maximum values on page 24.
April 16, 2019	Policy learning mode is not working as expected and has been removed from the new features list. Also, Bug ID 509835 has been moved from Resolved issues to Known issues.
February 25, 2019	Corrections to the section Product integration and support on page 24.
February 19, 2019	New section IPsec VPN features that are not supported on page 9.
February 11, 2019	Minor updates.
February 8, 2019	Initial version (for build 4214)

Introduction

This document provides the following information for FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261:

- Supported models
- What's new in FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261
- Special notices
- Upgrade information
- Product integration and support
- Resolved issues for build 4254
- Resolved issues for build 4214
- Known issues

Supported models

FortiGate-6000 v5.6.7 build 4261 supports the following models:

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

FortiGate-7000 v5.6.7 build 4261 supports all FortiGate-7030E, 7040E, and 7060E models and configurations.

What's new in FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261

FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261 includes the bug fixes described in Resolved issues for build 4261 on page 25 and Resolved issues for build 4254 on page 26. The first released build of FortiGate-6000 and FortiGate-7000 v5.6.7 was build 4214.

The following new features have been added to FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261:

- The FortiGate-6000 and FortiGate-7000 support 64000 explicit proxy web proxy users.
- The HA group ID range is now from 0 to 31 (was 0 to 15).

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 v5.6.7 build 4261.

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 the FortiGate-6000 handbook chapter 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 the FortiGate-7000 handbook chapter for detailed procedures for upgrading FortiGate-6000 firmware from the BIOS.

SD-WAN is not supported

FortiGate-6000 and FortiGate-7000 Version 5.6.7 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.
- Policy routes for VPN traffic.
- Remote networks with 0- to 15-bit netmasks.
- IPv6 clear-text traffic (IPv6 over IPv4 or IPv6 over IPv6).
- Load-balancing IPsec VPN tunnels to multiple FPMs.
- IPsec SA synchronization between both FortiGate-6000s in an HA configuration.

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 administration port numbers

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

Slot Number	Slot Address	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)
5	FPM05	8005	44305	2305	2205
3	FPM03	8003	44303	2303	2203
1	FIM01	8001	44301	2301	2201
2	FIM02	8002	44302	2302	2202
4	FPM04	8004	44304	2304	2204
6	FPM06	8006	44306	2306	2206

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 rules for how the FortiGate-6000 or FortiGate-7000 handles traffic types that cannot be load balanced. All of these flow rules identify the traffic type using the options available in the command and direct the traffic to the primary (or master) FPC or FPM. The rules also include a comment that identifies the traffic type.

Most of the flow rules are enabled (`status` set to `enable`) and they will direct matching traffic to the primary FPC. However, the configuration does include some disabled flow rules. You can enable these flow rules if required for your network.

The CLI syntax below was created with the `show` command and just shows the configuration changes. All other options are set to their defaults. Flow rules with no `status` option are disabled be default. Also the default `forward-slot` setting is `master`, which directs matching traffic to the primary FPC or FPM.

```
show load-balance flow-rule
config load-balance flow-rule
    edit 1
        set ether-type ip
        set protocol udp
        set src-l4port 88-88
        set comment "kerberos src"
    next
```

```
edit 2
    set ether-type ip
    set protocol udp
    set dst-l4port 88-88
    set comment "kerberos dst"
next
edit 3
    set status enable
    set ether-type ip
    set protocol tcp
    set src-l4port 179-179
    set comment "bgp src"
next
edit 4
    set status enable
    set ether-type ip
    set protocol tcp
    set dst-l4port 179-179
    set comment "bgp dst"
next
edit 5
    set status enable
    set ether-type ip
    set protocol udp
    set src-l4port 520-520
    set dst-l4port 520-520
    set comment "rip"
next
edit 6
    set status enable
    set ether-type ipv6
    set protocol udp
    set src-l4port 521-521
    set dst-l4port 521-521
    set comment "ripng"
next
edit 7
    set status enable
    set ether-type ipv4
    set protocol udp
    set src-l4port 67-67
    set dst-l4port 68-68
    set comment "dhcpv4 server to client"
next
edit 8
    set status enable
    set ether-type ipv4
    set protocol udp
    set src-l4port 68-68
    set dst-l4port 67-67
    set comment "dhcpv4 client to server"
next
```

```
    edit 9
        set ether-type ip
        set protocol tcp
        set src-l4port 1723-1723
        set comment "pptp src"
    next
    edit 10
        set ether-type ip
        set protocol tcp
        set dst-l4port 1723-1723
        set comment "pptp dst"
    next
    edit 11
        set status enable
        set ether-type ip
        set protocol udp
        set dst-l4port 3784-3784
        set comment "bfd control"
    next
    edit 12
        set status enable
        set ether-type ip
        set protocol udp
        set dst-l4port 3785-3785
        set comment "bfd echo"
    next
    edit 13
        set status enable
        set ether-type ipv6
        set protocol udp
        set src-l4port 547-547
        set dst-l4port 546-546
        set comment "dhcpv6 server to client"
    next
    edit 14
        set status enable
        set ether-type ipv6
        set protocol udp
        set src-l4port 546-546
        set dst-l4port 547-547
        set comment "dhcpv6 client to server"
    next
    edit 15
        set status enable
        set ether-type ipv4
        set dst-addr-ipv4 224.0.0.0 240.0.0.0
        set comment "ipv4 multicast"
    next
    edit 16
        set status enable
        set ether-type ipv6
        set dst-addr-ipv6 ff00::/8
```

```
        set comment "ipv6 multicast"
    next
    edit 17
        set ether-type ipv4
        set protocol udp
        set dst-l4port 2123-2123
        set comment "gtp-c to master blade"
    next
    edit 18
        set status enable
        set ether-type ipv6
        set protocol udp
        set dst-l4port 500-500
        set comment "ipv6 ike"
    next
    edit 19
        set status enable
        set ether-type ipv6
        set protocol udp
        set dst-l4port 4500-4500
        set comment "ipv6 ike-natt dst"
    next
    edit 20
        set status enable
        set ether-type ipv6
        set protocol esp
        set comment "ipv6 esp"
    next
    edit 21
        set status enable
        set ether-type ipv4
        set protocol udp
        set dst-l4port 500-500
        set comment "ipv4 ike"
    next
    edit 22
        set status enable
        set ether-type ipv4
        set protocol udp
        set dst-l4port 4500-4500
        set comment "ipv4 ike-natt dst"
    next
    edit 23
        set status enable
        set ether-type ipv4
        set protocol esp
        set comment "ipv4 esp"
    next
    edit 24
        set status enable
        set ether-type ip
        set protocol tcp
```

```
        set dst-l4port 1000-1000
        set comment "authd http to master blade"
    next
    edit 25
        set status enable
        set ether-type ip
        set protocol tcp
        set dst-l4port 1003-1003
        set comment "authd https to master blade"
    next
    edit 26
        set status enable
        set ether-type ip
        set protocol vrrp
        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 v5.6.7 build 4261.

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 5.6.7 build 4261 is supported from the following builds:

- FortiOS v5.6.6 build 4148 (FortiGate-6000)
- FortiOS v5.6.6 build 4184 (FortiGate-7000)
- FortiOS v5.6.7 build 4214

Upgrading a FortiGate-6000 or FortiGate-7000 HA cluster with `uninterruptable-upgrade` enabled is not supported from 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.

Possible heartbeat communication issue when upgrading an HA cluster

This issue does not apply to FortiGate-6000 or FortiGate-7030E HA configurations if you have set up direct connections between the HA heartbeat interfaces. For these models, the issue described in this section is only an issue if you have used switches to connect the HA heartbeat interfaces.

Problems can occur with HA heartbeat communication when upgrading a FortiGate-6000 or FortiGate-7000 HA configuration from FortiOS 5.4.x to FortiOS 5.6.6 if the switches used to connect the HA heartbeat interfaces are configured incorrectly. For FortiOS 5.6.6 and later, its mandatory to have switch ports configured in trunk mode to allow the heartbeat packets to pass through the switch.

The FortiOS 5.4.x FortiGate-6000 and FortiGate-7000 documentation described how to configure switches for HA heartbeat configuration. If you configured the switches correctly, after upgrading to FortiOS 5.6.6, HA heartbeat communication will still work. However, because of how FortiOS 5.4.x FortiGate-6000 and FortiGate-7000 HA heartbeat packets worked, it is possible to configure switches to allow FortiOS 5.4.x HA heartbeat packets but not allow FortiOS 5.6.6 HA heartbeat packets. Trunk mode wasn't strictly required for FortiOS 5.4.x. In this case, a FortiOS 5.4.x HA configuration could stop functioning after upgrading to FortiOS 5.6.6.

Verifying the status of an HA configuration after a firmware upgrade

After upgrading the firmware of a FortiGate-6000 or FortiGate-7000 HA configuration to FortiOS 5.6.7, the `get system ha status` command can show both FortiGate-6000s or FortiGate-7000s in the cluster even if the HA heartbeat switch configuration is incorrect.

However, if there is a problem with HA heartbeat communication, the `diagnose sys confsync status` command only shows the FPCs or FIMs/FPMs in a single chassis. If this occurs:

1. Verify that the switch port for each HA heartbeat interface has been configured as a trunk port. If not, enable trunk mode on the switch port. For example, for a Cisco switch, apply the setting `switchport mode trunk`.
2. Make sure the switch port's native VLAN ID is not the same as the heartbeat interface VLAN ID. Change the switch port's native VLAN ID if required.
3. If the switch port configuration is correct, and the `diagnose sys confsync status` command still shows only one chassis, its likely that the switch is stripping the inner VLAN tag. You could use a different switch or upgrade the licensing on the switch you are using to include Q-in-Q support.

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"
   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
```

FortiGate-6000 upgrade information

FortiGate-6000 v5.6.7 build 4261 supports upgrading from FortiGate-6000 v5.6.6 Build 4148 or from v5.6.7 build 4214 to v5.6.7 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 from 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 briefly be interrupted during the upgrade process. The entire firmware upgrade takes a few minutes, depending on the number of FPCs in your FortiGate-6000 system. Also, 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 the following:

- 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.
- Backup 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 everything 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 after the upgrade that you can still reach the server and that performance is comparable. You could also take a snapshot of key performance indicators (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 v5.6.7 build 4261 supports upgrading from FortiGate-7000 v5.6.6 Build 4184 or from v5.6.7 build 4214 to v5.6.7 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 from 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 briefly be interrupted during the upgrade process. The entire firmware upgrade will take a few minutes depending on the number of FIMs and FPMs in your FortiGate-7000 system. Also, 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 the following:

- 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.
- Backup 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 everything 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 after the upgrade that you can still reach the server and that performance is comparable. You could also take a snapshot of key performance indicators (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 5.6.7 release notes for product integration and support information for FortiGate-6000 and FortiGate-7000 v5.6.7.

Also please note the following exceptions for FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261:

Minimum recommended FortiManager firmware version : 6.0.5 and 6.2.0

Minimum recommended FortiAnalyzer firmware version : 6.0.5 and 6.2.0

FortiGate-6000 v5.6.7 special features and limitations

FortiGate-6000 v5.6.7 has specific behaviors that may differ from FortiOS features. For more information, see the "Special features and limitations for FortiGate-6000 v5.6.7" section of the most recent version of the FortiGate-6000 handbook for FortiOS 5.6.7: https://docs.fortinet.com/document/fortigate-6000/5.6.7/fortigate-6000-handbook.

FortiGate-7000 v5.6.7 special features and limitations

FortiGate-7000 v5.6.7 has specific behaviors that may differ from FortiOS features. For more information, see the "Special features and limitations for FortiGate-7000 v5.6.7" section of the most recent version of the FortiGate-7000 handbook for FortiOS 5.6.7: https://docs.fortinet.com/document/fortigate-7000/5.6.7/fortigate-7000-handbook.

Maximum values

Maximum values for FortiGate-6000 and FortiGate-7000 for FortiOS 5.6.7 are available from the FortiOS 5.6.7 Maximum Values Table.

Resolved issues for build 4261

The following issues have been fixed in FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261. 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 4254

The following issues have been fixed in FortiGate-6000 and FortiGate-7000 v5.6.7 build 4254. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
541234	FortiGate-7000 PSU information now displays correctly on the dashboard and the CLI.
545125 545275	Resolved an issue that blocked access to some interfaces if certain events (such as HA failovers or other changes) occur too often.
537732	Resolved an issue that caused system time to be set incorrectly.
550134	Resolved an issue that caused the `hatalk` process to use excessive amounts of CPU after enabling or disabling an FPC.
540310	Resolved an FPC memory leak found during internal testing.
540217	Resolved an issue that prevented the backup chassis in an HA configuration from contacting an NTP server.
544160 514677	Resolved two issues that caused ACD process crashes.
540668	Resolved an issue with long VDOM names that could cause config errors when loading a configuration file.
535397	The default antivirus quarantine destination has been changed from disk to null.
567551	Resolved an issue that caused the chlbd process CPU usage to reach 100%.
545670	The FortiGate-7000 DP processor no longer creates duplicate sessions.
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.
553301	Resolved an issue that caused the FortiGate-7000 to generate higher than expected numbers of `link_change` and `link_reinit` messages.
480307	IPS decoder configurations are now correctly converted when upgrading from v5.6.6 to v5.6.7.
536653	DP processor calendar rows are no longer mismatched between chassis in a FortiGate-6000 or FortiGate-7000 HA configuration.

Common vulnerabilities and exposures

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

Vulnerability
FortiGate-6000F and 7000F v5.6.7, build 4254, (GA) is no longer vulnerable to https://fortiguard.com/psirt/FG-IR-19-144.

Bug ID	CVE references
529745	FortiOS 5.6.7 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)
496642	FortiOS 5.6.7 for FortiGate-6000 and 7000 series is no longer vulnerable to the following CVE Reference: • CVE-2018-13371 (see: https://fortiguard.com/psirt/FG-IR-18-230)
529353	FortiOS 5.6.7 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 5.6.7 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 5.6.7 for FortiGate-6000 and 7000 series is no longer vulnerable to the following CVE Reference: • CVE-2019-5586 and CVE-2019-5588 (see: https://fortiguard.com/psirt/FG-IR-19-034)
529719	FortiOS 5.6.7 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 5.6.7 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 4214

The following issues have been fixed in FortiGate-6000 and FortiGate-7000 v5.6.7 build 4214. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
517951	Resolved an issue with synchronizing FSSO user group membership between FPMs.
517086	Error messages no longer appear while enabling FortiTokens.
528236	Resolved an issue with how numeric values appear on the CPU Usage dashboard widget.
526863	Resolved an issue with DP3 processor session handling that may cause traffic delays.
510862	Resolved an issue with IPsec VPN load balancing that resulted in duplicate tunnel IDs being created resulting is disrupted IPsec VPN sessions.
465295	The FortiGate-7060E supports synchronizing FortiClient licenses between its two Management Modules.
480280	Link failure control (configured with `config system interface set fail-detect enable`) now works as expected.
493920	SD-WAN rules now work as expected. However, volume-based SD-WAN load balancing is not supported.
496642	Some low level routing functionality is no longer visible.
502218	Resolved an issue that caused synchronization problems after changing an HA heartbeat interface VLAN ID.
502468	Resolved a TACACS+ authentication synchronization issue.
510613	The correct list of supported SD-WAN load balancing algorithms now appears on the GUI and CLI.
516041	The `config system settings set motherboard-traffic-forwarding auth` option has been removed.
518086	Fixed a typo in the get system status output.
518090	The `get system session` list command, when entered from the management board CLI, now only shows management board sessions, as intended.
518339	Resolved communication problems between some FortiGate-6000 and FortiGate-7000 components and configured FortiAnalyzers in a FortiGate-6000 or FortiGate-7000 HA configuration.
518764	Resolved an issue that sometimes prevented VLAN interface secondary IP addresses from being synchronized to all FPCs or FPMs.

Bug ID	Description
518814	The `diagnose sys ha history read` command now correctly displays information for both devices in an HA configuration.
519073	The `get system ha status` command now displays chassis information.
519139	Resolved a FortiGate-7000 issue with server load balancing communication to real servers when that traffic passes through a LAG interface that includes interfaces from two FIMs.
519309	SD-WAN options are now visible on the FortiGate-7000 GUI. However, SD-WAN is not currently supported.
520079	The `diagnose hardware ipmitool sensor` command and the `execute sensor list` command now correctly show all sensor data.
520191	Timestamps shown in sniffer captures is now correctly formatted as local time and not UTC time.
520732	Resolved a communication issue that prevented a FortiGate-6000 or FortiGate-7000 from being able to download firmware updates from FortiGuard.
522021	Resolved an internal duplicate MAC address issue.
522387	Resolved an issue with slot numbering in `get system ha status` command output.
522525	Resolved an issue that sometimes prevented the GUI from displaying memory logs.
522638	Resolved an issue that prevented a FortiGate-6000 or FortiGate-7000 information from functioning as an NTP server.
522788	Resolved an issue that caused the MAC address forwarding database (FDB) of a transparent mode VDOM to loose entries after a firmware upgrade with `uninterruptable-upgrade` enabled.
522799	Resolved a performance issue caused by SSL mirroring.
523173	The `diagnose load-balance switch stats non-zero` command now successfully clears all switch counters.
523566	Resolved an issue that caused the GUI or CLI to display the wrong model number after applying a FortiCarrier license.
524407	The GUI and CLI of both FIMs in a FortiGate-7000 now display the same memory log messages.
525484	Resolved an issue that sometimes prevented the front panel graphic from displaying on the **Network > Interfaces** GUI page.
525592	Resolved an issue that sometimes blocked communication with LDAP servers.
526030	Resolved an issue that sometimes caused an HA failover after a FortiGuard AV or IPS database update.
526168	Resolved an issue that sometimes caused synchronization problems after a FortiGuard update.

Bug ID	Description
526509	Resolved an issue that prevented the central management configuration from being synchronized.
526758	Management interfaces on the backup FortiGate-6000 or FortiGate-7000 in an HA configuration no longer accept traffic.
528236	CPU and memory usage displayed on dashboard widgets is now round off to one decimal point.
528760	Resolved an issue that could prevent administrators from adding FortiTokens.
529497	UTM information is now included in web-proxy traffic logs.
530363	Resolved an issue that caused a kernel crash when changing the disk RAID level.
531627	The GUI now displays HA status information correctly from the dashboard and the **System > HA** page.
532564	The `diagnose sys session clear` command no longer removes sessions that should not be cleared. For example, sniffer sessions and configuration synchronization sessions are no longer cleared by this command.
533051	The System Information dashboard widget now shows the correct serial number.
533124	Internal peer synchronization sessions are no longer synchronized to the backup FortiGate-6000 or FortiGate-7000 in an HA configuration.
533435	Stopping the packet sniffer from the primary FIM or the management board now also successfully stops the associated sniffer processes running on the FIMs and FPMs or the FPCs.
533453	HA failovers no longer occur after changing the `board-failover-tolerance` setting.
533775	Resolved an issue with the Security Fabric dashboard widget.

Known issues

The following issues have been identified in FortiGate-6000 and FortiGate-7000 v5.6.7 build 4261. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
534491	Random temporary throughput drops noticed by some customers.
537360	The interface dashboard widget may report incorrect outbound traffic numbers under some conditions, such as when UTM features and `auto-asic-offload` are enabled or when outgoing traffic contains small packets.
509835	Policy learning mode does not operate as expected.
531740	In some cases, known attack traffic may not be blocked by the IPS.
460967	The Unit Operation dashboard widget may not show accurate FPM or FPC session counts.
532094	Data ports may be unable to communicate FortiGuard.
528457	Performance issues related to the software switch feature.
530025	Routing tables may not be correctly synchronized between FPMs or FPCs.
527505	NP6 offloading cannot be disabled for FortiGate-6000 port 15 to 28 (100Gigbit interfaces).
475169	The `updated` process that downloads FortiGuard updates may crash while performing an IPS engine update.
501753	The IPS engine fail-open feature may cause repeated HA failovers while processing FortiGuard IPS updates.
444107	NFS v2/v3 over UDP mount actions through a FortiGate-6000 or FortiGate-7000 sometimes fail.
449298	FortiAnalyzer may not report correct FortiGate-6000 or FortiGate-7000 resource utilization.
530765	The `miglogd` logging process may crash due to a segmentation fault.
528496	The output from the `diagnose debug authd fsso list` command is inconsistent across FPCs or FPMs.