FORTINET

FortiGate-7000 Release Notes

VERSION v5.6.6 Build 4184

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 COOKBOOK

http://cookbook.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: techdocs@fortinet.com

February 11, 2019

FortiGate-7000 v5.6.6 build 4184 Release Notes

01-566-526013-20190211

TABLE OF CONTENTS

Change log

Date	Change description
February 11, 2019	New section Possible heartbeat communication issue when upgrading an HA cluster on page 17.
February 1, 2019	New section Limitations of installing FortiGate-7000 firmware from the BIOS after a reboot on page 8.
January 30, 2019	Minor updates.
December 20, 2018	Initial version.

Introduction

This document provides the following information for FortiGate-7000 v5.6.6 build 4184:

Supported models

FortiGate-7000 v5.6.6 build 4184 supports all FortiGate-7030E, 7040E, and 7060E models and configurations.

What's new in FortiGate-7000 v5.6.6 build 4184

Version 5.6.6 enhancements include adding FortiOS 5.6.6 to the FortiGate-7000 platform. This release also includes bug fixes and improvements and the following new features.

- Support for FortiOS 5.6.6 and most 5.6.6 features including FortiOS 5.6.6 GUI features.
- You can configure new Resource Usage dashboard widgets to show CPU use, log rate, memory use, session creation rate, and the number of active sessions for individual FIMs, the management plane, the data plan and the security fabric.
- The Security Fabric dashboard widget shows high level status and configuration information for all of the FPMs.
- The Sensor Information dashboard widget displays temperature information and allows you to drill down for information about individual temperature sensors.
- DP2 firmware upgrade
- VRRP support. For a list of know VRRP issues, see VRRP known issues on page 30.
- The management VDOM is now named mgmt-vdom (was dmgmt-vdom).
- The `diagnose sniffer packet` command now shows the name of the FPM that processed the packet.
- You can now use the `execute ping` and `execute traceroute` commands from an FIM CLI to an external destination.
- FIMs directly query LDAP/FSSO/RADIUS servers. These queries no longer have to go through the management VDOM.
- The Route Monitor displays accurate routing information.
- SNMP integration improvements including new MIBs.
- The following FortiOS 5.6.6 features are not supported:
  - SD-WAN
  - Some IPsec VPN features

- Policy learning mode
- HA dedicated management interfaces

New IPsec VPN features

FortiOS 5.6.6 includes the following IPsec VPN improvements:

- Including a phase 2 selector is no longer mandatory.
- Dynamic routing (RIP, OSPF, BGP) is supported over IPsec VPN tunnels.

IPsec VPN features supported by FortiOS 5.6.6 for FortiGate-7000

FortiOS 5.6.6 for FortiGate-7000 supports the following IPsec VPN features.

- Interface-based IPsec VPN (also called route-based IPsec VPN).
- Static routes can point IPsec VPN interfaces.
- Dynamic routing (RIP, OSPF, BGP) over IPsec VPN tunnels.
- Remote networks with 16- to 32-bit netmasks.
- IPsec VPN tunnels must terminate on the primary FPM (the ELBC master).
- Site-to-Site IPsec VPN.
- Dialup IPsec VPN. The FortiGate-7000 can be the dialup server or client.
- IPv4 clear-text traffic (IPv4 over IPv4 or IPv4 over IPv6)

IPsec VPN features not supported by FortiOS 5.6.6 for FortiGate-7000

FortiOS 5.6.6 for 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-7000s in an HA configuration.

New High Availability features and changes

Configuring FortiGate-7000 HA has been simplified for FortiOS 5.6.6. To set up HA, you no longer have to configure HA settings for both of the FIMs in a FortiGate-7000. Instead, you configure HA settings on the primary FIM and this configuration is synchronized to the other FIM.

As well, FortiGate-7000 HA is configured and operates more like standard FGCP HA. The link failure threshold concept that was part of FortiGate-7000 for FortiOS 5.4 has been removed and board failover tolerance has been simplified. As well, primary unit selection has been simplified to be more like FGCP primary unit selection.

FortiOS 5.6.6 also includes the following new features and changes:

- The **System > HA** GUI page now appears and can be used to configure most HA settings.
- You can configure HA interface monitoring (or port monitoring) to detect link failures.

- You can configure HA remote link failover (also called remote IP monitoring) to detect remote link failures using the following options:
  - Enable remote IP monitoring with the `pingserver-monitor-interface` option.
  - Set the remote IP monitoring failover threshold with the `pingserver-failover-threshold` option.
  - Force the cluster to negotiate after a remote IP monitoring failover with the `pingserver-slave-force-reset` option.
  - Adjust the time to wait in minutes before renegotiating after a remote IP monitoring failover with the `pingserver-flip-timeout` option.
- You can use the `get system ha status` command to display HA status. The `diagnose sys ha status` command is no longer available.
- The `diagnose sys ha force-slave-state` command is no longer available. To force the primary FortGate-7000 into a backup (or slave) state you can use the `diagnose sys ha reset-uptime` command.
- The HA `link-failure-threshold` option has been removed.
- The `board-failover-tolerance` option has been simplified and determines how the cluster responds to failed FIMs.

Special notices

This section highlights some of the operational changes that administrators should be aware of for FortiGate-7000 5.6.6 build 4184.

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

A common method for resetting the configuration of a FortiGate involves installing firmware by restarting the FortiGate, interrupting the boot process, and using BIOS prompts to download a firmware image from a TFTP server. This process is also considered the best way to reset the configuration of your FortiGate.

Installing or upgrading FortiGate-7000 firmware in this way 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.

To also reset all of the FIMs and FPCs, after installing firmware from the BIOS on the primary FIM, install the same firmware image from the GUI or from the CLI using the `execute restore image` command. This operation synchronizes the same firmware build and reset configuration to the FIMs and FPCs.

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

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-7000 platform.

Special configuration required for SSL VPN

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

```
config load-balance flow-rule
   edit 0
      set status enable
      set ether-type ipv4
      set protocol tcp
      set dst-l4port 10443-10443
      set forward-slot master
      set comment "ssl vpn server to primary FPM"
   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 FPM. This should match all of your SSL VPN traffic if you are using the default SSL VPN server listening port (10443). This flow rule also matches all other sessions using 10443 as the destination port so all of this traffic is also sent to the primary FPM.

Adding the SSL VPN server IP address

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

```
config load-balance flow-rule
   edit 26
      set status enable
      set ether-type ipv4
      set protocol tcp
      set dst-addr-ipv4 172.25.176.32 255.255.255.0
      set dst-l4port 10443-10443
      set forward-slot master
      set comment "ssl vpn server to primary FPM"
   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 FPM.

If you change the SSL VPN server listening port

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

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

Default configuration for traffic that cannot be load balanced

The default FortiGate-7000 `configure load-balance flow-rule` command contains the recommended default rules for how the 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) FIM. 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 FIM. 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 FIM.

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

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

```
        set protocol udp
        set src-l4port 68-68
        set dst-l4port 67-67
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv4 client to server"
    next
    edit 9
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 1723-1723
        set dst-l4port 0-0
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp src"
    next
    edit 10
        set status disable
        set vlan 0
        set ether-type ip
        set protocol tcp
        set src-l4port 0-0
        set dst-l4port 1723-1723
        set tcp-flag any
        set action forward
        set forward-slot master
        set priority 5
        set comment "pptp dst"
    next
    edit 11
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 3784-3784
        set action forward
        set forward-slot master
        set priority 5
        set comment "bfd control"
    next
    edit 12
        set status enable
        set vlan 0
        set ether-type ip
        set protocol udp
        set src-l4port 0-0
```

```
        set dst-l4port 3785-3785
        set action forward
        set forward-slot master
        set priority 5
        set comment "bfd echo"
    next
    edit 13
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 547-547
        set dst-l4port 546-546
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 server to client"
    next
    edit 14
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 546-546
        set dst-l4port 547-547
        set action forward
        set forward-slot master
        set priority 5
        set comment "dhcpv6 client to server"
    next
    edit 15
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 224.0.0.0 240.0.0.0
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 multicast"
    next
    edit 16
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ff00::/8
```

```
        set protocol any
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 multicast"
    next
    edit 17
        set status disable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 2123-2123
        set action forward
        set forward-slot master
        set priority 5
        set comment "gtp-c to master blade"
    next
    edit 18
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike"
    next
    edit 19
        set status enable
        set vlan 0
        set ether-type ipv6
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 ike-natt dst"
    next
    edit 20
        set status enable
        set vlan 0
        set ether-type ipv6
```

```
        set src-addr-ipv6 ::/0
        set dst-addr-ipv6 ::/0
        set protocol esp
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv6 esp"
    next
    edit 21
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 500-500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike"
    next
    edit 22
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol udp
        set src-l4port 0-0
        set dst-l4port 4500-4500
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 ike-natt dst"
    next
    edit 23
        set status enable
        set vlan 0
        set ether-type ipv4
        set src-addr-ipv4 0.0.0.0 0.0.0.0
        set dst-addr-ipv4 0.0.0.0 0.0.0.0
        set protocol esp
        set action forward
        set forward-slot master
        set priority 5
        set comment "ipv4 esp"
    next
    edit 24
        set status enable
        set vlan 0
        set ether-type ip
```

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

Upgrade information

FortiGate-7000 v5.6.6 build 4184 supports upgrading from any FortiGate-7000 5.4.9 release.

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.

Possible heartbeat communication issue when upgrading an HA cluster

This issue does not apply to FortiGate-7030E HA configurations if you have set up direct connections between the HA heartbeat interfaces. For the FortiGate-7030E, its only an issue if you have used switches to connect the HA heartbeat interfaces.

Problems can occur with HA heartbeat communication when upgrading aFortiGate-7000 HA configuration from FortiOS 5.4.9 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 5.4.9 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 5.4.9 FortiGate-7000 HA heartbeat packets worked, it is possible to configure switches to allow FortiOS 5.4.9 HA heartbeat packets but not allow FortiOS 5.6.6 HA heartbeat packets. Trunk mode wasn't strictly required for FortiOS 5.4.9. In this case, a FortiOS 5.4.9 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-7000 HA configuration to FortiOS 5.6.6, the `get system ha status` command can show both 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 FIMs and 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-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
```

Recommended firmware upgrade steps

Use the following steps to upgrade the firmware running on your FortiGate-7000 system from FortiOS 5.4.9 to 5.6.6:

1. Backup your FortiGate-7000 configuration.
2. Review the information in these release notes before starting the upgrade process.
3. If you are upgrading a FortiGate-7000 HA configuration, disable uninterruptible upgrade.
```
config system ha
   set uninterruptable-upgrade disable
end
```
This feature is not supported for upgrading from 5.4.9 to 5.6.6.
4. From the primary FIM CLI run the `diagnose sys confsync status` command to verify that the primary FIM can communicate and is synchronized with all FIMs and FPMs.
The command output should indicate `state=3(connected)` and `in_sync=1` for all modules. Including modules in the both FortiGate-7000s in an HA configuration.
5. Download the FortiGate-7000 5.6.6 firmware image from the Fortinet Support site.
6. Log into the primary FIM GUI or CLI and perform a normal firmware upgrade.
For example, from the GUI System Information dashboard widget select **Firmware Version > Update**.
From the CLI, use the `execute restore image <protocol> <image-file> ...` command.

7. Wait for the upgrade to complete.
   The upgrade will take a few minutes. For information about what to expect, how to determine the upgrade is complete, and what to do if something has gone wrong, see Upgrade to 5.6.6 may take longer than expected on page 20.

HA uninterruptable upgrade not supported

The FortiGate-7000 platform does not support the HA uninterruptable upgrade feature when upgrading a FortiGate-7000 HA cluster from FortiOS 5.4.9 to 5.6.6. To upgrade a Fortigate-7000 HA cluster to 5.6.6, you must first disable uninterruptable upgrade using the following command:

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

Once you have disabled uninterruptable upgrade you can proceed with a normal firmware upgrade of the HA cluster. However, the upgrade will disrupt network traffic, so perform the upgrade during a maintenance window.

By default, uninterruptable upgrade is disabled for the FortiGate-7000 series.

Upgrade to 5.6.6 may take longer than expected

Upgrading from FortiGate-7000 5.4.9 to v5.6.6 may take longer than expected because this firmware upgrade includes a DP2 processor firmware upgrade and because of renaming the management VDOM. These two changes happen automatically but add an extra internal step to the upgrade process that can take a few minutes. If you log into the CLI you can follow these steps of the upgrade process, see Sample message display during a normal upgrade on page 21.

To verify that the FIMs and FPMs are running the correct firmware version and to upgrade the firmware on individual modules if required:

1. After the firmware upgrade appears to be complete, log into the primary FIM and verify that it is running 5.6.6 firmware. You can verify the firmware version running on the primary FIM from the dashboard or by using the `get system status` command.
2. Log into the other FIMs and the FPMs and confirm that they are also running the correct 5.6.6 firmware.
   You can log into individual FIMs or FPMs using the system management IP address and the special port number for each module. For example, https://192.268.1.99:44303 connects to the module in slot 3. The special port number (in this case 44303) is a combination of the service port (for HTTPS the service port is 443) and the slot number (in this example, 03).
   If you are using a management module console port to connect to the primary FIM CLI you can use Ctrl-T to switch between the CLIs of each of the modules.
3. If an FIM is not running 5.6.6 firmware you can perform a normal firmware upgrade of the FIM from the GUI or CLI.
4. If an FPM is not running 5.6.6 firmware, you should run the following command from the primary FIM. For example, for the FPM in slot 3 enter:
   `diagnose load-balance switch set-compatible 3 enable elbc`

5. Log into the FPM GUI using its special port number (for example https://192.168.1.99:44303) and perform a normal firmware upgrade of the FPM.
6. Once the FPM restarts and you have verified that the correct firmware has been installed, you must to log back into the primary FIM and enter the following command to reset the FPM to normal operation.
   ```
   diagnose load-balance switch set-compatible 3 disable
   ```
   Configuration synchronization errors will occur if you do not reset the FPM to normal operation.
7. Continue in this way until you have verified and, if necessary, upgraded the firmware for each FIM and FPM.

You can also upgrade FIM or FPM firmware from the FIM or FPM BIOS. You can find information about how to do this in the FortiGate-7000 guide.

The dmgmt-vdom configuration migrates to mgmt-vdom

Upgrading to 5.6.6 will migrating your existing dmgmt-vdom configuration to the new mgmt-vdom management VDOM. All settings should be preserved and you should not have to re-do or change any configuration after the firmware upgrade is complete.

Sample message display during a normal upgrade

Messages similar to the following should appear on the primary FIM CLI console during the firmware upgrade process. If the DP image upgrade or the mgmt-vdom migration doesn't end successfully content Fortinet Support for assistance.

```
Upgrade output (the upgrade logs below for reference)
1) DP Upgrade output:
Firmware upgrade in progress ...
old:0x300 0x20170919 --- new:0x300 0x20180822
Update FortiASIC-DP Firmware.
Please don't power off during the update.....!
FortiASIC-DP update: Start process for chip 0
FortiASIC-DP update: Start process for chip 1
FortiASIC-DP.0: update file (/data/fpga.7910E.0300.20180822.rbf)
FortiASIC-DP update: Start process for chip 2
FortiASIC-DP.1: update file (/data/fpga.7910E.0300.20180822.rbf)
FortiASIC-DP.2: update file (/data/fpga.7910E.0300.20180822.rbf)
FortiASIC-DP.0: 0% Complete
FortiASIC-DP.2: 0% Complete
FortiASIC-DP.1: 0% Complete
FortiASIC-DP.2: 10% Complete
FortiASIC-DP.0: 10% Complete
FortiASIC-DP.1: 10% Complete
FortiASIC-DP.2: 20% Complete
FortiASIC-DP.0: 20% Complete
FortiASIC-DP.1: 20% Complete
FortiASIC-DP.2: 30% Complete
FortiASIC-DP.0: 30% Complete
FortiASIC-DP.1: 30% Complete
FortiASIC-DP.2: 40% Complete
```

```
FortiASIC-DP.0: 40% Complete
FortiASIC-DP.1: 40% Complete
FortiASIC-DP.2: 50% Complete
FortiASIC-DP.0: 50% Complete
FortiASIC-DP.1: 50% Complete
FortiASIC-DP.2: 60% Complete
FortiASIC-DP.0: 60% Complete
FortiASIC-DP.1: 60% Complete
FortiASIC-DP.2: 70% Complete
FortiASIC-DP.0: 70% Complete
FortiASIC-DP.1: 70% Complete
FortiASIC-DP.2: 80% Complete
FortiASIC-DP.0: 80% Complete
FortiASIC-DP.1: 80% Complete
FortiASIC-DP.2: 90% Complete
FortiASIC-DP.0: 90% Complete
FortiASIC-DP.1: 90% Complete
FortiASIC-DP.2: download complete.
FortiASIC-DP.2: update success (94.657578 s).
FortiASIC-DP.2: chip reconfigure, try again
FortiASIC-DP.0: download complete.
FortiASIC-DP.0: update success (95.061275 s).
FortiASIC-DP.0: chip reconfigure, try again
FortiASIC-DP.1: download complete.
FortiASIC-DP.1: update success (95.249837 s).
FortiASIC-DP.1: chip reconfigure, try again
FortiASIC-DP.2: chip reconfigure... success.
FortiASIC-DP.0: chip reconfigure... success.
FortiASIC-DP.0: update process finished with status 0
FortiASIC-DP.1: chip reconfigure... success.
FortiASIC-DP.1: update process finished with status 0
FortiASIC-DP.2: update process finished with status 0
DP image updated successfully!
DP image is upgraded successfully.
Done.

2) dmgmt-vdom migration output:
Press any key to display configuration menu...
.............................

Reading boot image 2827047 bytes.
Initializing firewall...
System is starting...
need a dmgmt-vdom migration process before configuration upgrade.
The config file may contain errors,
Please see details by the command 'diagnose debug config-error-log read'
dmgmt-vdom migrate completed.
```

Product integration and support

See the product integration and support section of the FortiOS 5.6.6 release notes for product integration and support information for FortiGate-7000 v5.6.6 build 4184.

Also note the following exceptions for FortiGate-7000 v5.6.6 build 4184:

Minimum recommended FortiManager firmware version: 5.6.7 and 6.0.4

Minimum recommended FortiAnalyzer firmware version: 5.6.7 and 6.0.4

FortiGate-7000 v5.6.6 special features and limitations

FortiGate-7000 v5.6.6 has specific behaviors which may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000 v5.6.6 section of the most recent version of the FortiGate-7000 Handbook chapter available at https://docs.fortinet.com/document/fortigate/5.6.6/fortigate-7000.

Resolved issues

The following issues have been resolved in FortiGate-7000 v5.6.6 build 4184. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
416207	SNMP queries now successfully poll all of the modules in an FortiGate-7000 system.
422404	FPM to FortiAnalyzer and FPM to remote syslog server communication now works correctly if `source-ip` is set.
441228	RADIUS/FSSO/LDAP status information displayed on the GUI is now accurate.
465295	In a FortiGate-7060E system, FortiClient and other licenses are now synchronized between both shelf managers.
470485	Routing Monitor results are now correct.
471943	Application names are now connect in saved crash logs.
478360	IPv6 VIPs successfully translate IP addresses.
478749	FortiView historical data display works as expected.
480280	Link failure control works as expected.
484733	Setting the interface media type to LR is now supported for all FIMs. Previously the LR setting on some FIMs would be lost after a reboot.
487066	MAC addresses for the ".b" interfaces in Transparent mode VDOMs are now synchronized.
491123	VDOM setting under central-management should not allow VDOMs other than dmgmt-vdom
491417	FortiGate is dropping server hello packets when urlfilter is enabled.
492601	Add 'Out of Sync' indicate to csf if member out of sync.
493052	Sometimes slave blade lost kernel static route after bringing down/up traffic interface.
493106	Disable store-and-upload option for log to FortiAnalyzer and FortiGuard.
493656	IPsec tunnel status should be listed on management board.
493929	The primary (or master) FIM shows the correct FSSO connection status for the FPMs.
494441	Mismatch lag members and min-link value.

Bug ID	Description
496206	TP VDOM is failed to create if CSF is enabled.
496463	Sometimes static routes are missing in VWL VDOM.
498058	chassis-HA out-of-sync due to cached checksum missed calculate.
499249	Ingress-trunk-mapping from FIM01 and FIM02 are not matched, and caused NAT traffic fail.
500226	You can use the `diagnose load-balance set slot currrent` command to prevent the `get system performance status` command from displaying performance status for all modules.
500535	LAG configuration settings are now correctly synchronized to FPMs even if it changes many times.
501672	BFD neighbors are not coming up when BFD is configured on the fly.
502137	Upgrade issue cause ips.json missing.
502443	LR mediatype inft failed to change speed from 100G to 40G.
502468	TACACS+ authentication works from FPMs but not FIMs.
504104	get router info bgp summary send wrong command to slave.
504305	Increase IPv6 route cache sizes.
504732	DP weighted-load-balance does not work.
505041	The link status are not synced on all blades.
505307	Decode VDOM license key failed.
505837	FPMs no longer fail to resolve available DNS servers.
506593	VLAN RUNNING flag is not consistent after trunk administrative down.
506732	Config antivirus quarantine does not allow disk to be configured as destination.
507269	Newly inserted blade should re-obtain the FortiClient license from SMM.
507340	Dashboard Widget for aggregate Management & Dataplane CPU Utilization, Sessions & Memory.
507492	Hide A-A mode from the GUI.
507972	HA failover of TCP sessions now works as expected. The DP processor no longer forwards TCP sessions to the wrong FPM.

Bug ID	Description
508670	Fix session sync IP issue when changing HA mode.
509140	Memory logs not always generated for IPv6 DoS attacks.
509390	Can't display Quarantine Monitor screen in GUI.
509716	Fix fortiview data might list without aggregated.
509721	Fix drill down issues in FortiView.
509736	USG licenses are now successfully synchronized to all FPMs.
509835	Hide learning report from 7k.
509908	vsys_ha VDOM shouldn't have any proto=18/20 routes.
510316	The primary FIM now displays accurate antivirus statistics.
510550	Failed to retrieve information for 'sd-wan' interface.
510613	The list of supported load balancing algorithms for sd-wan is different from CLI.
510758	Fix top source widget failed to show data.
510763	FortiView failed to drill down to details.
510798	Resolved an issue that caused FPMs to get out of sync after a configuration change.
510821	Fix FortiView VPN IPsec issue.
510830	Some options should remove from mgmt-vdom.
512058	Check first 6 characters of sn to make sure it is the same chassis type to form HA cluster.
512085	Dual register FortiClient to FGT and EMS, deregister all can't clear the FortiClient.
512515	Re-enabling CLI debugs not working properly.
512617	The `get router info bfd neighbor/requests` command now displays the expected information on all FIMs and FPMs.
512792	CMD 'get system ha ha-mgmt-interfaces' should be hidden.
513039	Fix dataplane widgets aggregate number issues.
513042	Show per slot usage if dataplane selected.
513477	Fix ha device empty change when modify device location.

Bug ID	Description
513678	Sensor response is malformatted message printed.
513679	The `diagnose sys ntp status` command no longer displays status information for all on the FPMs.
513690	all mgmt interfaces should be able to handle local out traffic at the same time.
513962	FortiView list data flickering reduced.
514091	The `diagnose sys kill` command only stops processes on the module on which it is entered.
514108	Disable wireless-controller sections have been removed from FortiView.
514335	Bring UP/Down functions now work as intended on the IPsec Monitor.
514498	Report setting, fmg send command unset pdf-report/ unset FortiView, status no change.
514818	Dialup ipsec vpn not listed in Monitor->IPsec Monitor page.
514929	HA hbdev and monitor inft missing in the HA setting.
515234	Confsync packet should not be able to get through HA front port HA1/HA2 when mode is changed to standalone.
515722	mgmt-vdom should not be able to change opmode (no TP mode supported for mgmt-vdom).
515905	7K unit not displaying several SNMP objects (1.3.6.1.4.1.12356.101.13.2.1).
516255	The primary FIM now displays FortiAnlyzer log messages for all FIMs and FPMs.
516620	IPsec tunnel interface is down causing the traffic can't be sent out via tunnel interface to trigger the tunnel negotiate.
517316	GUI HA faceplate failed to display.
517319	GUI Dashboard -> Security Fabric widget only show current blade status.
517637	FEC feature is missing in FIM7920E.
518327	No data for widgets Sessions, Session Rate, CPU, Memory for the dataplane.
518452	QSFP+ 40G interface speed change failed to take effect on BCM switch.
518746	7KE should be able to access if only 2-mgmt interfaces are connected.
519001	HA flap was noticed when FGT-7K having larger serial number joins an existing HA cluster that has been up for long time.

Bug ID	Description
519340	Support span sniffer on 7KE.
521520	Not able to View FSSO User groups from FAC(Collector Agent) in Standard Mode.
522638	NTP response on any Interface shows Clock Unsynchronized and NTP Clients are unable to get the Correct time.
522788	Mac fib of a transparent VDOM is not synced during uninterruptible-upgrade.
523173	"diagnose load-balance switch stats non-zero" failed to clear some switch counters.
523566	After applied FortiCarrier license, the model number has changed to 6000F.
523785	Concurrent Explicit Proxy User Number is smaller for on a FortiGate-7000 compared to a FortiGate-3700D.
524407	Support Integrated memory log for FGT-7000E.
525592	LDAP server configuration does not work on one of the vdom, getting error "ldap_-3".

Known issues

The following issues have been identified in FortiGate-7000 v5.6.6 build 4184. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
517951	FSSO user group membership may be out of sync between FPMs.
514159	Interface faceplate not displayed on the GUI for administrators without the super_admin administrator profile.
520281	Certificate Revocation Lists (CRL) added to a VDOM may be deleted because of synchronization errors. You can work around this issue by adding the CRL to the global configuration.
459424	Statistics displayed on the **System > VDOM** page may be incorrect.
527567	IPsec VPN tunnels may fail after an HA failover because routes used by the VPN are not available on the new primary unit.
526863	Intermittent performance reduction for Link Aggregation (LAG) groups that include interfaces from multiple FIMs.
526030	An HA failover may occur after an antivirus database update.
524128	Interface media type changes (SR/LR) may not be synchronized by HA, so after a failover some of the interfaces of the new primary unit may be operating with the incorrect media type.
517905	SNMP configurations on individual FPMs may have different `snmp-index` settings.
526393	Overriding the global syslog server for individual VDOMs does not work and individual VDOMs use the global syslog server.
524841	Responses to SNMP queries by the primary FIM may time out after six seconds, even if the system is not very busy.
521421	When the FortiGate-7000 is configured to detect devices on attached networks, the `src-vis` process may use excessive amounts of CPU resources.
525612	IPv6 `execute ping6` and `execute traceroute6` commands don't work from FIM console.
525619	Cannot stop IPv4 ping or traceroute sessions initiated from FIM console. To stop a ping or traceroute session you must lot out of the CLI.

IPsec VPN known issues

Bug ID	Description
528797	Learned dynamic routes with subnet mask lengths larger than 16 will be added to VPN DP route table as 16-bit routes.
528800	Duplicate routes appear in the DP routing table if the system receives the same route from different IPsec VPN tunnels.
526531	With an ADVPN configuration, the BFD debug report may display `Network is unreachable` messages.
527039	OSPF packets are not sent from the dialup server to dialup clients over the dialup IPsec interface.
527035	ADVPN shortcut tunnels can't be established when the tunnel is triggered by the FortiGate-7000 system.
523755	Different dialup IPsec tunnels with the same name but created on different FPMs will not appear in the IPsec VPN tunnel list.

VRRP known issues

Bug ID	Description
524721	VRRP state mismatch between master FIM and slave FIM of HA master chassis.
524452	VRRP failover is not happening when vrdst ip address is not reachable.
524414	VRRP start-time is not working; It always takes the default value of 3 seconds irrespective of value configured.