FortiGate-7000 - Release Notes

Version 5.4.9 Build 8110

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

December 20, 2019
FortiGate-7000 5.4.9 Build 8110 Release Notes
01-549-505860-20191220

TABLE OF CONTENTS

Change log

Date	Change description
December 20, 2019	New information added to IPsec VPN phase 2 selectors on page 7.
August 23, 2018	Initial version.

Introduction

This document provides the following information for FortiGate-7000 v5.4.9 build 8110:

Supported models

FortiGate-7000 v5.4.5 build 8110 supports all FortiGate-7030E, 7040E, and 7060E models and configurations.

What's new in FortiGate-7000 v5.4.9 build 8110

Version 5.4.9 enhancements mainly consisted of adding FortiOS 5.4.9 to the FortiGate-7000 platform. This release also includes bug fixes and improvements and one additional new feature.

Brief logging mode

Brief logging mode, a carrier grade NAT (CGN) feature, removes some fields from log messages to reduce log message size. Smaller log messages reduces disk space usage and also reduces remote logging network bandwidth usage. Brief logging mode is useful if your FortiGate-7000 system generates a large amount of log messages.

Use the following command to enable brief logging mode for all logging:

```
config log setting
   set brief-traffic-format enable
end
```

Special notices

This section highlights some of the operational changes that administrators should be aware of for FortiGate-7000 5.4.9 build 8110.

Limitations of installing FortiGate-6000 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-6000 firmware in this way 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.

To also reset the FPCs, after installing firmware from the BIOS on the management board, 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 FPCs.

You could also manually install firmware on each individual FPC from the BIOS after a reboot but this manual process will not be more effective than installing the firmware for a second time on the management board to trigger synchronization to the FPCs.

Special configuration required for SSL VPN

Using a FortiGate-6000 as an SSL VPN server requires you to manually add an SSL VPN load balance flow rule to configure the FortiGate-6000 to send all SSL VPN sessions to the primary (master) FPC. 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 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 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
```

IPsec VPN phase 2 selectors

FortiGate-7000 IPsec VPNs require phase 2 selectors. The phase 2 selectors specify the IP addresses and netmasks of the source and destination subnets of the VPN. The phase 2 selectors are mandatory on the FortiGate-7000 and are used to make sure that all IPsec VPN traffic is sent to the primary (master) FPM.

Use the following command to add phase 2 selectors.

```
config vpn ipsec phase2-interface
```

```
edit "to_fgt2"
   set phase1name <name>
   set src-subnet <IP> <netmask>
   set dst-subnet <IP> <netmask>
end
```

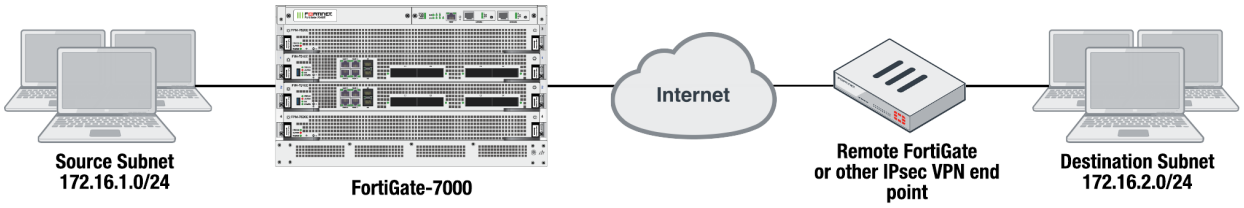
Where

`src-subnet` the subnet protected by the FortiGate that you are configuring and from which users connect to the destination subnet.

`dst-subnet` the destination subnet behind the remote IPsec VPN endpoint.

Example basic IPsec VPN phase 2 configuration

In a simple configuration such as the one below with an IPsec VPN between two remote subnets you can add the phase 2 selectors by adding the subnets to the phase 2 configuration as shown.

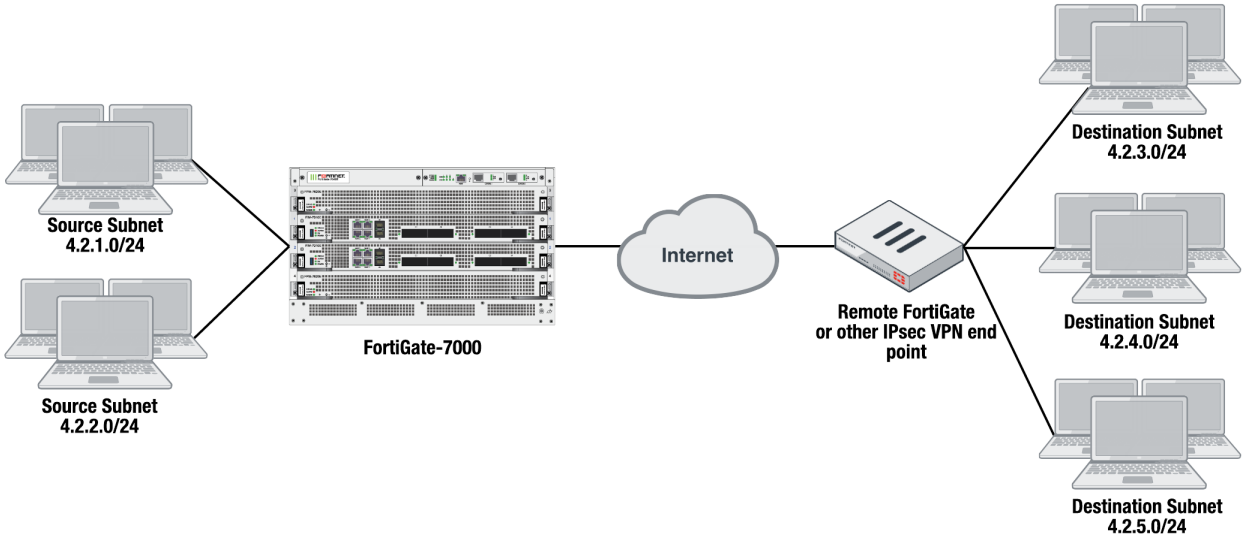


Enter the following command to add the source and destination subnets phase 2 selectors to the FortiGate-7000 IPsec VPN Phase 2 configuration.

```
config vpn ipsec phase2-interface
   edit "to_fgt2"So
      set phase1name "to_fgt2"
      set src-subnet 172.16.1.0 255.255.255.0
      set dst-subnet 172.16.2.0 255.255.255.0
   end
```

Example multiple subnet IPsec VPN phase 2 configuration

In a more complex configuration, such as the one below with a total of 5 subnets you still need to use the phase 2 selectors to add all of the subnets to the Phase 2 configuration. In this case you can create a firewall address for each subnet, add the addresses to address groups, and add the address groups to the phase 2 selectors.



Enter the following commands to create firewall addresses for each subnet.

```
config firewall address
   edit "local_subnet_1"
      set subnet 4.2.1.0 255.255.255.0
   next
   edit "local_subnet_2"
      set subnet 4.2.2.0 255.255.255.0
   next
   edit "remote_subnet_3"
      set subnet 4.2.3.0 255.255.255.0
   next
   edit "remote_subnet_4"
      set subnet 4.2.4.0 255.255.255.0
   next
   edit "remote_subnet_5"
      set subnet 4.2.5.0 255.255.255.0
   end
```

And then put the five firewall addresses into two firewall address groups.

```
config firewall addrgrp
   edit "local_group"
      set member "local_subnet_1" "local_subnet_2"
   next
   edit "remote_group"
      set member "remote_subnet_3" "remote_subnet_4" "remote_subnet_5"
   end
```

Now, use the firewall address groups in the Phase 2 configuration:

```
config vpn ipsec phase2-interface
   edit "to-fgt2"
      set phase1name "to-fgt2"
      set src-addr-type name
      set dst-addr-type name
      set src-name "local_group"
```

```
      set dst-name "remote_group"
   end
```

Recommended configuration for traffic that cannot be load balanced

The following flow rules are recommended to handle common forms of traffic that cannot be load balanced. These flow rules send GPRS (port 2123), SSL VPN, IPv4 and IPv6 IPsec VPN, ICMP and ICMPv6 traffic to the primary (or master) FPM.

The CLI syntax below just shows the configuration changes. All other options are set to their defaults. For example, the flow rule option that controls the FPM slot that sessions are sent to is `forward-slot` and in all cases below `forward-slot` is set to its default setting of `master`. This setting sends matching sessions to the primary (or master) FPM.

```
config load-balance flow-rule
   edit 20
      set status enable
      set ether-type ipv4
      set protocol udp
      set dst-l4port 2123-2123
   next
   edit 21
      set status enable
      set ether-type ip
      set protocol tcp
      set dst-l4port 10443-10443
      set comment "ssl vpn to the primary FPM"
   next
   edit 22
      set status enable
      set ether-type ipv4
      set protocol udp
      set src-l4port 500-500
      set dst-l4port 500-500
      set comment "ipv4 ike"
   next
   edit 23
      set status enable
      set ether-type ipv4
      set protocol udp
      set src-l4port 4500-4500
      set comment "ipv4 ike-natt src"
   next
   edit 24
      set status enable
      set ether-type ipv4
      set protocol udp
      set dst-l4port 4500-4500
      set comment "ipv4 ike-natt dst"
   next
   edit 25
      set status enable
```

```
        set ether-type ipv4
        set protocol esp
        set comment "ipv4 esp"
    next
    edit 26
        set status enable
        set ether-type ipv6
        set protocol udp
        set src-l4port 500-500
        set dst-l4port 500-500
        set comment "ipv6 ike"
    next
    edit 27
        set status enable
        set ether-type ipv6
        set protocol udp
        set src-l4port 4500-4500
        set comment "ipv6 ike-natt src"
    next
    edit 28
        set status enable
        set ether-type ipv6
        set protocol udp
        set dst-l4port 4500-4500
        set comment "ipv6 ike-natt dst"
    next
    edit 29
        set status enable
        set ether-type ipv6
        set protocol esp
        set comment "ipv6 esp"
    next
    edit 30
        set ether-type ipv4
        set protocol icmp
        set comment "icmp"
    next
    edit 31
        set status enable
        set ether-type ipv6
        set protocol icmpv6
        set comment "icmpv6"
    next
    edit 32
        set ether-type ipv6
        set protocol 41
    end
```

Upgrade information

FortiGate-7000 v5.4.9 build 8110 supports upgrading from any FortiGate-7000 v5.4.5 release.

All of the modules in your FortiGate-7000 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 of all of the modules in the chassis upgrades in one step. Firmware upgrades should be done during a quiet time because traffic will briefly be interrupted during the upgrade process.

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 HA configuration.
- Review the services provided by your FortiGate-7000 before the 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 a key 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 .

Upgrading FortiGate-7000 HA cluster firmware

Fortinet recommends upgrading your FortiGate-7000 HA configuration firmware with `uninterruptable-upgrade` enabled. With `uninterruptable-upgrade` enabled, the FortiGate-7000 HA configuration goes through a multi-step process to upgrade the firmware of all components in the configuration. Since many components are involved, the entire upgrade process may take a few minutes. It all happens automatically and should cause only minor traffic disruptions. Because of the possible disruptions, you should upgrade HA cluster firmware when traffic is low or during a maintenance period.

Use the following command to enable uninterruptable-upgrade:

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

The following steps happen in the background when upgrading the firmware running on a FortiGate-7000 HA cluster with `uninterruptable-upgrade` enabled.

- The firmware upgrade downloads to the primary (master) FortiGate-7000.
- The primary FortiGate-7000 sends a copy of the firmware upgrade file to the backup (slave) FortiGate-7000.
- The backup FortiGate-7000 upgrades its firmware, restarts, and rejoins the cluster.
- The primary FortiGate-7000 verifies that all members of the backup FortiGate-7000 can process traffic. The firmware upgrade will not proceed until all of the backup FortiGate-7000 components are operating.
- The primary FortiGate-7000 then sends a switchover command and the backup FortiGate-7000 becomes the primary FortiGate-7000.
- The new primary FortiGate-7000 sends gratuitous ARP packets to inform attached network devices to send packets to the new primary FortiGate-7000.

- Traffic switches over to the new primary FortiGate-7000.
- The original primary FortiGate-7000 upgrades its firmware, restarts, and rejoins the cluster as the backup FortiGate-7000.

The amount of time this process takes and the probability of minor traffic disruptions depends on the number of modules in your FortiGate-7000 and on traffic load conditions, the network configuration, and how quickly the gratuitous ARP packets update network devices.

Product integration and support

See the product integration and support section of the FortiOS 5.4.9 release notes for product integration and support information for FortiGate-7000 v5.4.9 build 8110.

Also note the following exceptions for FortiGate-7000 v5.4.9 build 8110:

Minimum recommended FortiManager firmware version: (not currently available, these release notes will be updated when support is available)

Minimum recommended FortiAnalyzer firmware version: (not currently available, these release notes will be updated when support is available)

FortiGate-7000 v5.4.9 special features and limitations

FortiGate-7000 v5.4.9 has specific behaviors which may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000 v5.4.9 section of the most recent version of the FortiGate-7000 Handbook chapter available at http://docs.fortinet.com/d/fortigate-7000.

Maximum values

Maximum values for FortiGate-7000 for FortiOS 5.4.9 are available from https://help.fortinet.com/fgt/54/max-values/5-4-9/max-values.html.

Resolved issues

The following issues have been resolved in FortiGate-7000 v5.4.9 build 8110. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
507262	Resolved an issue that sometimes caused administrator account synchronization problems between modules.
505948	Resolved an administrator login context issue that could cause the output of the `diagnose sys confsync status` to include error messages.
496432	SNMP traps are now successfully generated and log message are generated when a chassis power supply fails.
507175	Redundant interface health status now displays correctly.
506256	The IP addresses used for communication between modules across the chassis backplane now update correctly after changing the chassis ID.
505910	Resolved an issue that resulted in dropped packets for traffic on a link aggregation group (LAG) containing interfaces from two FIM modules.
505041	FPMs no longer display MAC address errors after factory resetting the secondary chassis in an HA configuration.
504732	The weighted load balancing feature now works correctly.
504713	Resolved an issue that caused some load balanced transparent mode VDOM traffic to be dropped.
504196	Crash logs are no longer deleted after a firmware upgrade.
504036	Resolved an issue that displayed IPS syntax errors on the console after upgrading to v5.4.9.
503457	The System Information dashboard widget now correctly displays HA status information.
503451 488537 487066 484733	Interface attributes such as virtual MAC addresses and flags are now successfully synchronized to all FIM modules when in HA mode.
502988	The minimum MTU size of all FIM interfaces is now 256.
502613	The `get system status` command now shows correct information about the primary (master) FPM in an HA configuration.
502463	Resolved an issue that caused the `fctrlproxyd` process to appear busy and prevent interface status data from being synchronized.
502215	Resolved an issue that caused temporary synchronization problems if an administrator added, edited, or deleted the Interface History dashboard widget.
502137	Resolved an issue that prevented the secondary chassis in an HA configuration from synchronizing after a firmware upgrade.
502117	Removed hidden interfaces from various interface display pages.

Bug ID	Description
501630	Resolved an issue that caused the output of the `diagnose debug app slbhad 256` command to display incorrect interface status information.
500080	Clear text VPN traffic load balancing is no longer disrupted after adding or removing interfaces from a LAG.
499522	Resolved an issue that caused firmware upgrades of an HA configuration to take longer than expected with `uninterruptible-upgrade` enabled.
499479	De-authentication of FSSO users is now successfully synchronized to all FPMs.
499371	All FIMs now display LAG interface status correctly.
499249	Resolved an ingress trunk mapping issue that caused some NAT sessions to fail.
499214	Resolved an issue that could prevent firewall policy pages from displaying when operating in HA mode.
499095 474588 472277	Resolved issues that prevented FIM interface traffic history dashboard widgets from displaying accurate traffic data.
499084	Traffic accepted by a firewall policy is now correctly displayed on the secondary FIM firewall policy list.
498920	Resolved an issue that caused an HA failover after creating a new LAG interface.
498850	Error messages no longer appear after creating a firewall policy.
498532 498514	Resolved some issues with the `execute load-balance slot reboot` command.
498273	The HA configuration page now displays correctly formatted HA mode information.
497978	The `confsynccmdd` process no longer causes excessive CPU usage, resulting in inter-chassis synchronization errors.
497190	Resolved an issue that blocked access to the mgmt interface after changing its interface IP address.
492717	`wtp-profiles` are now correctly synchronized.
0491610	In an HA configuration, the interface monitor no longer displays incorrect information after bringing a LAG interface down.
491123	Central management can now only be configured for the dmgmt-vdom VDOM.
490866	The link-status of an interface on the secondary chassis in an HA configuration is no longer shown differently by the GUI and CLI.
488361	HA priority configuration changes are now correctly synchronized.
488336	Internal CSF sessions no longer reset unexpectedly.
486951	Certificates are now correctly synchronized in an HA configuration.
485496	Routes are now correctly synchronized to the primary (or master) FPM.
482639	Resolved an issue that could sometimes cause an firmware upgrade to fail for a FortiGate-7000 HA configuration with uninterruptable-upgrade enabled if the primary (or master) FIM changed during the upgrade.
481995	Traffic to and from the base-mgmt interface is no longer logged as denied.

Bug ID	Description
476921	Corrections to LLDP handling.
471832	Increased the IPv6 route cache limit to improve IPv6 performance in transparent mode.
471380	Corrected the output of the `get system checksum status` command.
462662	Event logs and SNMP traps are generated when an FIM or FPM is removed or inserted.
455825	Resolved an issue that prevented the FortiGuard auto-update feature from working as expected.
455790	The `get system transceiver` command now shows the status for the transceivers in all FIMs.
452266	A new FortiOS Carrier license is now successfully synchronized to all modules in a chassis.
441741	`dhcp-relay` options can now be configured for FIM interfaces.
439103	FortiClient licenses are now synchronized to all modules in a chassis.
424112	Event logs and SNMP traps are generated for PSU and cooling fan events.
415910	Resolved an issue that could cause CPU utilization being displayed as 0 when CPU utilization is high.
408693	Error messages no longer appear on some FortiView pages.
370881	Resolved an issue that caused the logging system to consume excessive amounts of memory.
463677	Resolved an issue that caused configuration synchronization may fail after creating a new administrator account.
501198	Resolved an issue that prevented the FortiGate-7040E from maintaining six million sessions under certain taffic conditions.

Known issues

The following issues have been identified in FortiGate-7000 v5.4.9 build 8110. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
501764	FortiGate-7000 v5.4.9 is not currently supported by FortiManager and FortiAnalyzer. Support will be added to a future FortiManager and FortiAnalyzer release.
385136	The M1 and M2 interface LEDs light after inserting certain transceivers, whether or not the transceiver is connected to a network.
506472	Shutting down an interface that is part of a LAG mail cause a failover. This occurs because the interface appears to be disconnected so the LAG has fewer links. You can work around this issue by removing the interface from the LAG before shutting it down.
460967	The Unit Operation widget does not accurately show the number of sessions running on all FPM modules.
501753	Under very high traffic conditions, the IPS fail open and cause cluster flapping .
502119	In some cases, DLP does not block PDF and PPT files over Google drive.
444107	NFS v2/v3 mount over UDP may fail.
502343	On an FIM, the `diagnose load-balance switch cmd` command output shows increasing `Sw_Tx_Drop_Packets` and `Sw_Rx_Drop_Packets` counters.
449298	FortiAnalyzer reports incorrect FortiGate-7000 resource utilization information.
493475	Error messages appear on the Firewall Address GUI page.
422404	FPMs cannot communicate with the configured FortiAnalyzer if the `source-ip` is set to the IP address of a management interface.
459424	The VDOM list GUI page does not show correct CPS, CPU, and memory usage for each VDOM.
489949	FIMs may send RTP (UDP/9000) traffic intermittently to the wrong FPM.
459413	HA remote IP monitoring using the `pingserver-monitor-interface`, `pingserverfailover-threshold`, and `pingserver-flip-timeout` does not work.
493850	GTP traffic statistics are not displayed correctly for the mgmt interface.
414651	Data displayed by some `diagnose` commands is not synchronized to all modules.
491439	The `route-ttl` option is missing for the HA configuration.
404811	Dynamic routing entries display incorrectly on the Routing Monitor.
441228	Adding an LDAP server from any FIM may fail because the FortiGate-7000 can't communicate with the LDAP server to test the connection. The workaround is to add the LDAP server from an FPM.