FortiGate-7000 Release Notes

VERSION v5.4.5 Build 8047

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

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

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

August 13, 2018

FortiGate-7000 v5.4.5 build 8047 Release Notes

01-545-452473-20180813

TABLE OF CONTENTS

Change log

Date	Change description
August 13, 2018	Added issue number 385136 to Known issues on page 18.
June 26, 2018	Updated for build 8047.
December 20, 2017	Initial version for build 6481.

Introduction

This document provides the following information for FortiGate-7000 v5.4.5 build 8047:

Supported models

FortiGate-7000 v5.4.5 build 8047 supports all FortiGate-7030E, 7040E, and 7060E models and configurations. Build 8047 introduces support for the FortiGate-7060E-8-DC.

What's new in FortiGate-7000 v5.4.5 build 8047

The following new features have been added:

The maximum value for user groups has been increased to 5,000 (460857)

On a FortiGate-7000, you can now configure up to 5,000 user groups.

Log field extension policy-name and meta-field (461783 455441)

An option to include the policy name field has been added to traffic logs (log-policy-name). An option to add a meta-field tag to all logs has also been added (custom-field and custom-log-fields; see below). This meta-field could be used to identify the FortiGate sending the logs, for example:

```
config log setting
   set log-policy-name enable
end
config log custom-field
   edit "cust-field"
      set name "MyFortiGate"
      set value "111"
   next
   end
      config log setting
      set custom-log-fields "cust-field"
   end
```

M1 and M2 interfaces can use different VLANs for heartbeat traffic (408386)

The M1 and M2 interfaces can be configured to use different VLANs for HA heartbeat traffic. Normally you would separate the M1 and M2 traffic. In that case you don't have to change their VLAN IDs. But if the M1 and M2 interfaces are connected to the same switch and you can't separate their traffic, or if you can't use the default VLAN IDs you can set a different VLAN ID for each interface.

Use the following command set the M1 and M2 interfaces to use different VLANs:

```
config system ha
   set hbdev M1/M2
   set hbdev-vlan-id 991
   set hbdev-second-vlan-id 992
end
```

For this configuration to work the `hbdev-vlan-id` has to be changed. You cannot use the default value of 999.

GTP load balancing

GTP load balancing is supported for FortiGate-7000 configurations licensed for FortiOS Carrier. You can use the following command to enable GTP load balancing. This command is only available after you have licensed the FortiGate-7000 for FortiOS Carrier.

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

FSSO user authentication synchronization

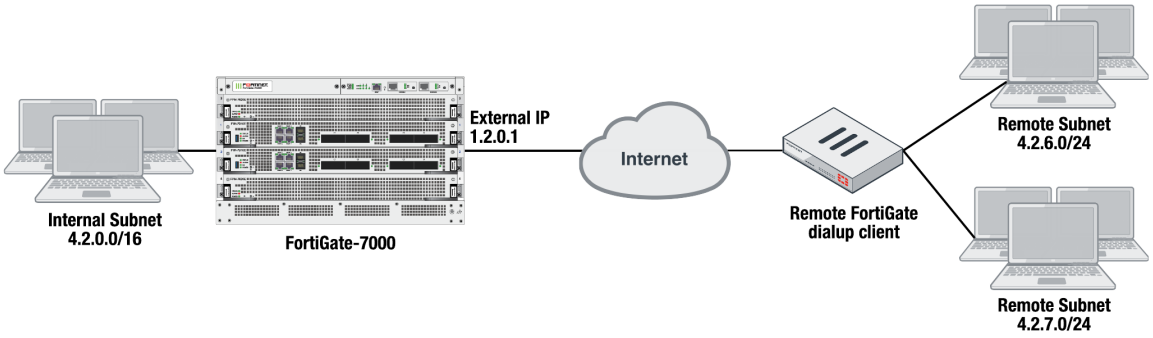
FSSO user authentication is synchronized to all FPM modules. Users authenticated through FSSO no longer have to re-authenticate when load balancing distributes their session to a different FPM module.

HA link failure threshold changes (422264)

The link failure threshold is now determined based on the all FIM modules in a chassis. This means that the chassis with the fewest active links will become the backup chassis.

FortiGate-7000s running FortiOS v5.4.5 can be configured as dialup IPsec VPN servers

The following shows how to setup a dialup IPsec VPN configuration where the FortiGate-7000 running v5.4.5 acts as a dialup IPsec VPN server.



Configure the phase1, set type to dynamic.

```
config vpn ipsec phase1-interface
   edit dialup-server
      set type dynamic
      set interface "v0020"
      set peertype any
      set psksecret < password>
   end
```

Configure the phase 2, to support dialup IPsec VPN, set the destination subnet to 0.0.0.0 0.0.0.0.

```
config vpn ipsec phase2-interface
   edit dialup-server
      set phase1name dialup-server
      set src-subnet 4.2.0.0 255.255.0.0
      set dst-subnet 0.0.0.0 0.0.0.0
   end
```

To configure the remote FortiGate as a dialup IPsec VPN client

The dialup IPsec VPN client should advertise its local subnet(s) using the phase 2 src-subnet option.

If there are multiple local subnets create a phase 2 for each one. Each phase 2 only advertises one local subnet to the dialup IPsec VPN server. If more than one local subnet is added to the phase 2, only the first one is advertised to the server.

Dialup client configuration:

```
config vpn ipsec phase1-interface
   edit "to-fgt7k"
      set interface "v0020"
      set peertype any
      set remote-gw 1.2.0.1
      set psksecret <password>
   end
config vpn ipsec phase2-interface
   edit "to-fgt7k"
      set phase1name "to-fgt7k"
      set src-subnet 4.2.6.0 255.255.255.0
      set dst-subnet 4.2.0.0 255.255.0.0
   next
   edit "to-fgt7k-2"
```

```
    set phase1name "to-fgt7k"
    set src-subnet 4.2.7.0 255.255.255.0
    set dst-subnet 4.2.0.0 255.255.0.0
end
```

Special notices

This section highlights some of the operational changes that administrators should be aware of for FortiGate-7000 5.4.5 build 8047.

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 v5.4.5 build 8047 supports upgrading from any FortiGate-7000 v5.4.5 release.

All of the modules in your FortiGate-7000 chassis run the same firmware image. You can upgrade the firmware by using the management IP address to log into the primary interface module GUI or CLI and perform a firmware upgrade just as you would for 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 is briefly interrupted during the upgrade process.

Upgrading FortiGate-7000 HA cluster firmware

Even with `uninterruptable-upgrade` enabled, upgrading a FortiGate-7000 HA configuration may cause a minor traffic disruption. You should upgrade HA cluster firmware when traffic is low or during a maintenance period.

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 FortiGate-7000.
- The primary FortiGate-7000 sends a copy of the firmware upgrade file to the backup FortiGate-7000.
- The backup FortiGate-7000 upgrades its firmware, restarts, and rejoins the cluster.
- The primary FortiGate-7000 fails over and the backup FortiGate-7000 switches to become the primary FortiGate-7000. During failover, the new primary FortiGate-7000 sends gratuitous ARP packets to inform attached network devices to send packets to the new primary FortiGate-7000.
- The original primary FortiGate-7000 upgrades its firmware, restarts, and rejoins the cluster as the backup FortiGate-7000.

Depending on traffic load conditions, the network configuration, and how quickly the gratuitous ARP packets update network devices there could be minor traffic disruptions during this upgrade process.

IPsec VPN issues when upgrading from v5.4.3 to v5.4.5

If your FortiGate-7000 configuration includes IPsec VPNs you should enhance your IPsec VPN Phase 2 configurations as described in this section.

Because the FortiGate-7000 only allows 16-bit to 32-bit routes, you must add one or more destination subnets to your IPsec VPN phase 2 configuration for FortiGate-7000 v5.4.5 using the following command:

```
config vpn ipsec phase2-interface
   edit "to_fgt2"So
      set phase1name <name>
      set src-subnet <IP> <netmask>
      set dst-subnet <IP> <netmask>
   end
```

Where

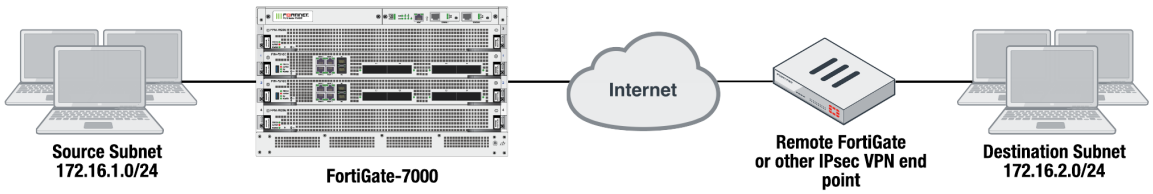
`src-subnet` the subnet protected by the FortiGate that you are configuring and from which users connect to the destination subnet. Configuring the source subnet is optional but recommended.

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

You can add the source and destination subnets either before or after upgrading to v5.4.5 as these settings are compatible with both v5.4.3 and v5.4.5. However, if you make these changes after upgrading, your IPsec VPNs may not work correctly until these configuration changes are made.

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 just add the subnets to the phase 2 configuration.

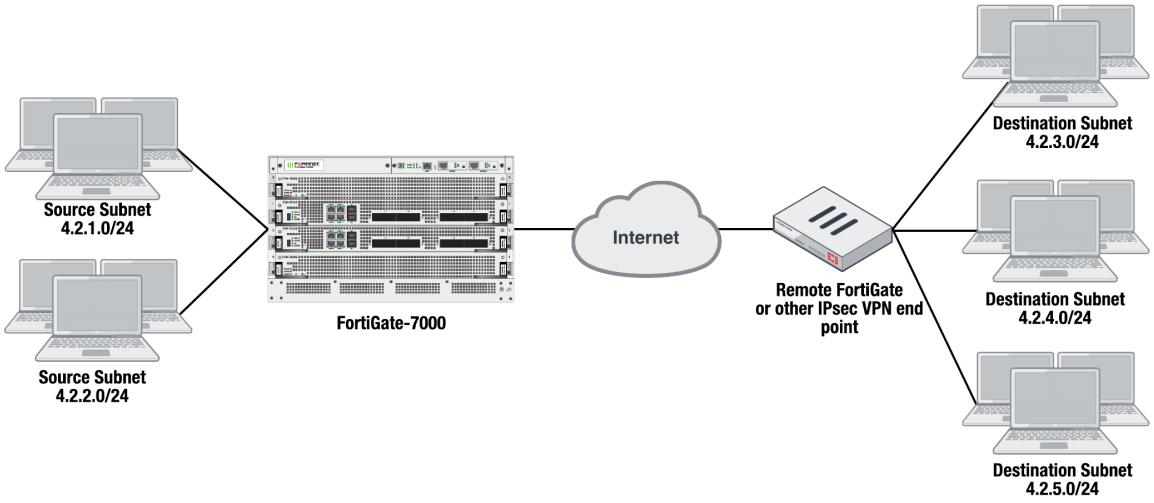


Enter the following command to add the source and destination subnets to the FortiGate-7000 IPsec VPN Phase 2 configuration.

```
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 add all of the subnets to the Phase 2 configuration. In this case you can create a firewall address for each subnet and the addresses to address groups and add the address groups to the Phase 2 configuration.



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
```

Product integration and support

See the product integration and support section of the FortiOS 5.4.5 release notes for product integration and support information for FortiGate-7000 v5.4.5 build 8047.

Also please note the following exceptions for FortiGate-7000 v5.4.5 build 8047:

Minimum recommended FortiManager firmware version : 5.6.5

Minimum recommended FortiAnalyzer firmware version : 5.4.4

FortiGate-7000 v5.4.5 special features and limitations

FortiGate-7000 v5.4.5 has specific behaviors which may differ from FortiOS features. For more information, see the Special features and limitations for FortiGate-7000 v5.4.5 section of the most recent version of the FortiGate-7000 Handbook chapter available at http://docs.fortinet.com/d/fortigate-7000.

Resolved issues

The following issues have been fixed in FortiGate-7000 v5.4.5 build 8047. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
479165	Fixed an issue that reduced GTP throughput performance.
461783 445374	The DSCP IP header field should not be changed for sessions processed by the SIP proxy.
459425	FortiView now displays sessions processed by all FPM modules.
458987	Fixed various issues that caused HA heartbeat failures.
459102	Fixed an issue that blocked communication with the management IP address after an HA failover.
476812	Fixed an issue that caused some nTurbo sessions to be dropped.
476757	Fixed an issue that prevented FortiClient for iPhone and FortiClient for Android from connecting to SSL VPN tunnels hosted by the FortiGate-7000.
472561	Fixed an issue that could cause a kernel panic after a factory reset.
476574	Backup FPM kernel routes on the new primary FortiGate-7000 now update correctly after an HA failover.
476973	Fixed an issue that caused packet loss through a VDOM operating in transparent mode.
301547 441068	Fixed an issue that kept inactive SSL VPNs in the session table for an extended period of time.
442365	FortiGate-7000 v5.4.5 build 6517 is no longer vulnerable to the following CVE-Reference: - CVE-2017-7738 Visit https://fortiguard.com/psirt for more information
464156	Fixed an issued that applied the wrong VLAN tags to HA heartbeat traffic.
464735	Decode VDOM license key failed error messages no longer appear when FortiGate-7000 components start up.
462228	NAT sessions are no longer dropped from DP timers problems after a system restart.
455825	FortiGuard auto-update no longer keeps contacting FortiGuard to request updates after a successful update.
460289	Authenticated users are synchronized to all FPMs. Users no longer have to re-authenticate if the FortiGate-7000 load balances their sessions to a different FPM.
454070	In an HA configuration, IPv4 routes are now correctly synchronized to all FPMs.

Bug ID	Description
456140	In an HA configuration, only the primary FIM module communicates with FortiManager.
456116	History output of the `diagnose sys ha status` command now includes timestamps to show when a failover occurred.
422602	In an HA configuration, failovers no longer occur after an antivirus update.
452415	The output of the `diagnose sys link-monitor status` command is now synchronized.
454411	Local certificates are now synchronized to all FIM modules.
453285	VLAN Traffic continues to flow through LAG interfaces between two FIMs if one of the FIMs is shut down.
448131	Incorrect link local IPv6 addresses that caused IPv6 traffic slowdowns have been corrected.
410647	Support added for TCP, HTTP, and UDP-based link monitoring for SD-WAN link load balancing.
423946	The `cmdbsvr` process no longer crashes when 500 VDOMs and 10k policies have been added.
439398	The `diagnose vpn ssl list` command now correctly displays information for all FIM and FPM modules.
442607	Changes to replacement messages made from a VDOM can now be successfully saved.
415234	You can set the Interface to any when creating a firewall VIP.
410741	AntiVirus, Web Filtering, and other security profile log messages generated by FPM modules now appear on the GUI of all FIM or FPM modules (including the GUI of the primary FIM module).
417584	HA chassis failover from management links only occurs if no management links are available on the chassis. As long as at least one management link is available a failover will not occur.
424015	Fixed a bug with firmware updates with `uninterruptable-upgrade` enabled that caused extra chassis failovers.
408535	The hostname is now synchronized to all modules.
392288	A configuration that includes 500 VDOMs can now be restored from the GUI.
488336	Fixed an issue that would periodically cause Security Fabric sessions to reset.
485496	Fixed a routing issue that prevented the primary FPM from getting the correct default route; resulting in problems with management connections to the primary FPM.
476921	Fixed an issue that caused LLDP information to be incorrect. Work to fix other LLDP related issues continues.
488537	Fixed a problem with gratuitous ARP support that caused attached network devices to get incorrect MAC addresses of some management interfaces.

Bug ID	Description
488361	Fixed an issue that prevented HA device priority changes from being synchronized correctly.
474387	The Firewall policy page now shows correct sessions, packets, and bytes data for each policy.
486559	Fixed an issue that caused the `chlbd` process to use 99% of the CPU and cause an HA cluster to become unstable.
484213	Fixed an issue that caused extra flow rules to be added after upgrading from FortiOS 5.4.3 to FortiOS 5.4.5. These extra flow rules resulted in uneven traffic distribution.

Known issues

The following issues have been identified in FortiGate-7000 v5.4.5 build 8047. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
385136	The M1 and M2 interface LEDs light after inserting certain transceivers, whether or not the transceiver is connected to a network.
444107	Remote NFS v2/v3 over UDP disk share mounting through a FortiGate-7000 fails. To work around this issue use NFS over TCP.
440550	Some FortiView pages may display "Failed to get FortiView" data error messages.
460148	Unreadable application field in system event log crash messages.
459413	HA remote IP monitoring using the `pingserver-monitor-interface`, `pingserver-failover-threshold`, and `pingserver-flip-timeout` does not work.
459424	The VDOM list GUI page does not show correct CPS, CPU, and memory usage for each VDOM.
442168	Traffic counters that display interface traffic for a physical interface do not display traffic sent and received by VLANs added to the physical interface.
422404	FPMs cannot communicate with the configured FortiAnalyzer if the `source-ip` is set to the IP address of a management interface.
449298	FortiAnalyzer reports incorrect FortiGate-7000 resource utilization information.
491945	The `sslvpnd` process may consume a high amount of CPU resources.
489131	Missing information in `diagnose debug rating` command output on the primary FIM.
484203	Management access to some FPMs and FIMs may be lost because of configuration synchronization issues.
482639	In an HA configuration, the backup FortiGate-7000 may not successfully upgrade to the new firmware version.
460967	The Unit Operation widget does not accurately show the number of sessions running on all FPM modules.
485485	In an active-passive HA configuration, the backup FortiGate-7000 may record error messages after FortiGuard updates even though the updates complete successfully.
471943	Crash log messages may contain incorrect application names.
481830	An FPM CLI may display a message similar to `protocol 0000 is buggy`.

Bug ID	Description
463677	Configuration synchronization may fail after creating a new administrator account.
460148	System event crash logs may not include the name of the application that crashed.
456872	Routing changes not synchronized to backup FPM modules after moving an LACP LAG interface into a new VDOM.
449298	FortiAnalyzer reports may contain incorrect FortiGate-7000 resource utilization information.
441228	Adding an LDAP server from the GUI may fail because the FortiGate-7000 can't communicate with the LDAP server to test the connection.
441741	DHCP relay configuration options missing from the CLI.