



# Hyperscale Firewall - Release Notes

Version 6.2.7 Build 7105

**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/training-certification>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



January 11, 2023

Hyperscale Firewall 6.2.7 Build 7105 Release Notes

01-627-708415-20230111

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Hyperscale firewall for FortiOS 6.2.7 release notes</b>	<b>5</b>
Supported FortiGate models	5
<b>What's new</b>	<b>6</b>
BGP IPv6 conditional route advertisement	6
BGP IPv6 conditional route advertisement configuration example	6
CGN session timeout improvements	7
Host logging syslog improvements	8
Hardware logging extended to session helpers and ALGs	9
Hardware logging log rate dashboard widget	9
Support for up to sixteen hardware logging servers	9
Hash table entry spread	10
HPE enhancements	10
Modifying trap session behavior in hyperscale firewall VDOMs	10
Bandwidth control for NPU accelerated VDOM link interfaces	11
Controlling the maximum outgoing VLAN bandwidth	11
Distribute HA session synchronization packets to multiple CPUs	12
SNMP improvements	12
SNMP queries for hardware session counts	12
SNMP queries for NAT46 and NAT64 policy statistics	13
SNMP queries of NP7 fgProcessor MIB fields	14
Maximum number of hyperscale firewall policies increased	16
<b>Special notices</b>	<b>17</b>
Check the NP queue priority configuration after a firmware upgrade	17
FortiGates with NP7 processors and NetFlow domain IDs	19
HPE limitations	19
Hyperscale firewall 6.2.7 incompatibilities and limitations	19
About hairpinning	20
Interface device identification is not compatible with hyperscale firewall traffic	21
<b>Upgrade information</b>	<b>22</b>
To upgrade an HA cluster from an older firmware version	22
To upgrade a standalone FortiGate from an older firmware version	23
<b>Product integration and support</b>	<b>24</b>
Maximum values	24
<b>Resolved issues</b>	<b>25</b>
<b>Known issues</b>	<b>29</b>

# Change log

Date	Change description
January 11, 2023	Added more information about <code>arp-reply</code> support limitations for IPv4 and IPv6 firewall VIPs to <a href="#">Hyperscale firewall 6.2.7 incompatibilities and limitations on page 19</a> .
February 14, 2022	New section: <a href="#">Check the NP queue priority configuration after a firmware upgrade on page 17</a> . Also, a note has been added about this issue to, <a href="#">Upgrade information on page 22</a> .
December 2, 2021	Added two new FGCP HA-related limitations to <a href="#">Hyperscale firewall 6.2.7 incompatibilities and limitations on page 19</a> .
October 18, 2021	Removed the incorrect statement "NP7 fragment reassembly is not supported" from <a href="#">Hyperscale firewall 6.2.7 incompatibilities and limitations on page 19</a> . See <a href="#">Reassembling fragmented packets</a> for information about supporting NP7 fragment reassembly.
August 23, 2021	Added known issue 740225 to <a href="#">Known issues on page 29</a> .
June 23, 2021	Added known issue 725975 to <a href="#">Known issues on page 29</a> .
June 21, 2021	Added information about FortiGates licensed for hyperscale firewall features not supporting the <code>proxy</code> option for DoS policy anomalies to <a href="#">Hyperscale firewall 6.2.7 incompatibilities and limitations on page 19</a> .
June 1, 2021	Initial version.

# Hyperscale firewall for FortiOS 6.2.7 release notes

These platform specific release notes describe new features, special notices, upgrade information, product integration and support, resolved issues, and known issues for FortGates licensed for Hyperscale firewall features for FortiOS 6.2.7 Build 7105.

In addition, special notices, new features and enhancements, changes in CLI defaults, changes in default values, changes in table size, product integration and support, resolved issues, known issues, and limitations described in the [FortiOS 6.2.7 Release Notes](#) also apply to FortGates licensed for Hyperscale firewall features for FortiOS 6.2.7 Build 7105.

For Hyperscale firewall documentation for this release, see the [Hyperscale Firewall Guide](#).

## Supported FortiGate models

Hyperscale firewall for FortiOS 6.2.7 Build 7105 supports the following models. The information in these release notes applies to these FortiGate models if they are licensed for Hyperscale firewall features.

- FortiGate-1800F
- FortiGate-1801F
- FortiGate-2600F
- FortiGate-2601F
- FortiGate-4200F
- FortiGate-4201F
- FortiGate-4400F
- FortiGate-4401F

# What's new

The following new features have been added to Hyperscale firewall for FortiOS 6.2.7 Build 7105. The changes in the CLI, changes in GUI behavior, changes in default behavior, changes in table size, and new features or enhancements are described in the [New features or enhancements](#) in the [FortiOS 6.2.7 release notes](#) also apply to Hyperscale firewall for FortiOS 6.2.7 Build 7105.

## BGP IPv6 conditional route advertisement

IPv6 BGP conditional route advertisement is a new feature that supports traffic failover for a FortiGate with hyperscale firewall features operating as a CGNAT translator connected to two ISPs over IPv6.

When the FortiGate can connect to the primary ISP, IPv6 BGP routes to the primary ISP are shared with the networks (LANs) behind the FortiGate. With BGP IPv6 conditional route advertisement enabled, if the FortiGate connection to the primary ISP fails, the FortiGate acquires IPv6 BGP routes to the secondary ISP and advertises these routes to the networks (LANs) behind the FortiGate.

Use the following configuration to enable IPv6 conditional route advertisement:

```
config router bgp
  config neighbor
    edit <name>
      config conditional-advertise6
        edit <name>
          set condition-routemap <name>
          set condition-type {exist | non-exist}
        end
      end
```

`exist` true if condition route map is matched.

`non-exist` true if condition route map is not matched.

## BGP IPv6 conditional route advertisement configuration example

The following configuration shows how to use the `condition-type` option to control how a FortiGate advertises routes when it is connected to two external routers.

When `condition-type` is set to `non-exist` the FortiGate advertises route2 (2003:172:22:1::/64) to Router2 when it learns route1 (2003:172:28:1::/64). When `condition-type` is set to `exist`, the FortiGate will not advertise route2 (2003:172:22:1::/64) to Router2 when it knows route1 (2003:172:28:1::/64).

```
config router prefix-list6
  edit adv-222
    config rule
      edit 1
        set prefix6 2003:172:22:1::/64
      end
```

```
config router prefix-list6
```

```
edit list6-1
  config rule
  edit 1
    set prefix6 2003:172:28:1::/64
  end

config router route-map
edit map-222
  config rule
  edit 1
    set match-ip6-address adv-222
  end
config router route-map
edit "map-281"
  config rule
  edit 1
    set match-ip6-address list6-1
  end
config router bgp
set as 65412
set router-id 1.1.1.1
set ibgp-multipath enable
set network-import-check disable
set graceful-restart enable
config neighbor
edit 2003::2:2:2:2
  set soft-reconfiguration6 enable
  set remote-as 65412
  set update-source loopback1
  config conditional-advertise6
  edit map-222
    set condition-routemap map-281
    set condition-type {exist | non-exist}
  end
edit 2003::3:3:3:3
  set soft-reconfiguration6 enable
  set remote-as 65412
  set update-source loopback1
end
```

## CGN session timeout improvements

FortiOS 6.2.7 supports enhancements for controlling CGN session timeouts. In addition to improvements in how session timeouts are controlled, the following command now applies to hyperscale firewall carrier grade NAT sessions. Using this command you can define a session timeout for a specific protocol and port range.

```
config system session-ttl
config port
edit 1
  set protocol <protocol-number>
  set timeout <timeout>
  set refresh-direction {outgoing | incoming | both}
  set start-port <port>
  set end-port <port>
```

end

`protocol <protocol-number>` a protocol number in the range 0 to 255. Default 0.

`timeout <timeout>` the time in seconds after which a matching idle session is terminated. Range 1 to 2764800. Default 300.

`refresh-direction {outgoing | incoming | both}` control whether idle outgoing or incoming or both outgoing and incoming sessions are terminated when the timeout is reached. This option is new for FortiOS 6.2.7.

`start-port <port>/end port <port>` the start and end ports in the range of ports that this session timeout configuration applies to. Range is 0 to 65535. Default is 0.



The `config system session-ttl` command is a VDOM command, configured from a VDOM. However, there is a known issue that options set by this command apply to all CGNAT VDOMs and not just the VDOM in which they are set.

---

## Host logging syslog improvements

FortiOS 6.2.7 syslog host logging sends log messages to syslog servers added to the hardware logging configuration. This release includes a number of host logging changes, including bug fixes and performance improvements.

You no longer have to support host logging to syslog servers by adding syslog servers with the `config log syslogd` command. The host logging syslog configuration is now the same as the standard hardware logging configuration. This new feature also usually results in improved syslog host logging performance.

Example syslog host logging configuration to use host logging to send log messages to a remote syslog server.

```
config log npu-server
  set log-processor host
  config server-info
    edit 1
      set vdom "root"
      set ipv4-server 55.55.55.55
      set source-port 8055
      set dest-port 2055
      set template-tx-timeout 60
    end
  end
  config server-group
    edit "log_ipv4_server1"
      set log-format syslog
      set server-number 1
      set server-start-id 1
    end
  end
end
```

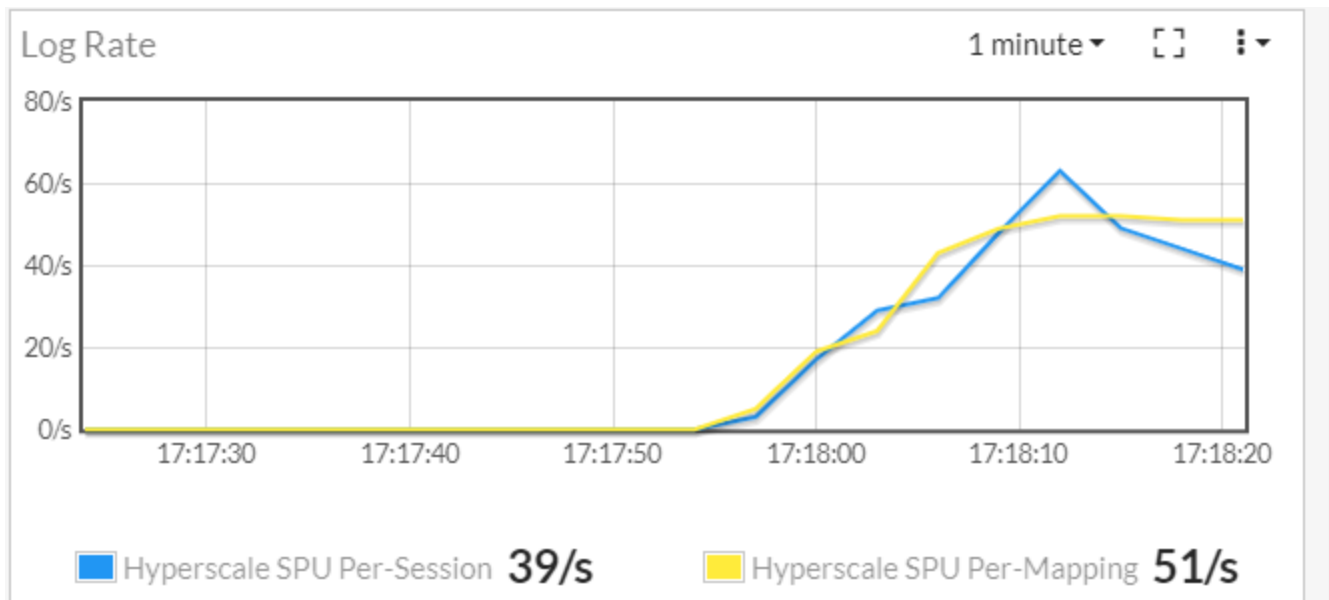
## Hardware logging extended to session helpers and ALGs

FortiOS 6.2.7 supports hyperscale firewall hardware logging for protocols that use session helpers or application layer gateways (ALGs). If hyperscale firewall policies accept session helper or ALG traffic, such as ICMP, hardware log messages for these sessions are created and sent according to the hardware logging configuration for the policy.

Previously, log messages for session helper or ALG traffic would be created by the CPU and handled according to the standard FortiOS logging configuration.

## Hardware logging log rate dashboard widget

On a FortiGate with a hyperscale firewall license, the Log Rate dashboard widget shows hardware logging log message creation rates. The widget shows the average hyperscale per-session and per mapping log message creation rates for the NP7 processors (SPUs) in the FortiGate.



You can also click on the widget to access hardware logging settings.

## Support for up to sixteen hardware logging servers

You can now include up to sixteen log servers in a log server group. In the following configuration, `<index>` under `config server-info` can be in the range of 1 to 16.

```
config log npu-server
  set log-processor {hardware | host}
  set netflow-ver {v9 | v10}
  config server-info
    edit <index>
```

## Hash table entry spread

You can use the following command to enable or disable hash table entry spread for NP7 processors.

```
config system npu
  set hash-tbl-spread {disable | enable}
end
```

hash-table-spread is enabled by default. In most cases hash-table-spread should be enabled.

The following diagnose commands have been added to allow monitoring VLAN + LAG accounting when hash-tble-spread is enabled:

```
diagnose npu np7 sse-tpe-accounting {enable|disable}
diagnose npu np7 vlan-accounting {enable | disable}
```

## HPE enhancements

The NP7 host protection engine (HPE) configuration has been enhanced with the addition of two new options:

```
config system npu
  config hpe
    set tcpsyn-ack-max 6000
    set tcpfin-rst-max 3000
  end
```

tcpsyn-ack-max <packets-per-second> prevent SYN\_ACK reflection attacks by limiting the number of TCP SYN\_ACK packets received per second. The range is 1000 to 40000000 pps. and the default is 600000. TCP SYN\_ACK reflection attacks occur when an attacker sends large amounts of SYN\_ACK packets without first sending SYN packets. These attacks can cause high CPU usage because the FortiOS firewall assumes that these SYN\_ACK packets are the first packets in a session, so the packets are processed by the CPU instead of the NP7 processors.

tcpfin-rst-max <packets-per-second> limit the maximum number of TCP FIN and RST packets received per second. The range is 1000 to 40000000 pps. and the default is 600000.

## Modifying trap session behavior in hyperscale firewall VDOMs

Hyperscale VDOMs now create trap sessions for all sessions that need to be handled by the CPU. Trap sessions make sure CPU sessions are successfully sent to the CPU. If CPU sessions are not trapped, they may be incorrectly converted to hardware sessions and dropped.

You can use the following command to modify trap session behavior in a hyperscale firewall VDOM

```
config system settings
  set trap-session-flag {udp-both | udp-reply | tcpudp-both trap | tcpudp-reply | trap-
    none}
end
```

udp-both trap UDP send and reply sessions.

udp-reply trap UDP reply sessions only.

`tcpudp-both` trap TCP and UDP send and reply sessions. This is the default setting.

`tcpudp-reply` trap TCP and UDP reply sessions only.

`trap-none` disable trapping sessions.

The default setting creates trap sessions for all TCP and UDP sessions to be handled by the CPU. You can change the trap session behavior depending on CPU sessions processed by the VDOM.

## Bandwidth control for NPU accelerated VDOM link interfaces

NP7 processors include a module called the Virtual Egress Processor (VEP) that processes all traffic that passes through NPU accelerated VDOM link interfaces, including interfaces that have been added to NPU accelerated VDOM link interfaces (for example VLANs).

You can improve overall performance by keeping accelerated VDOM link interfaces from consuming excessive NP7 bandwidth. By default, VEP now imposes the following maximum bandwidth allocations on NPU accelerated VDOM link interfaces:

- Maximum bandwidth supported across an NPU accelerated VDOM link with multiple sessions is 200Gbps.
- Maximum bandwidth supported across an NPU accelerated VDOM link with one session is 100Gbps.

You can use the following command to change the VEP mode:

```
diagnose npu np7 vep-mode {100G-2 | 100G | 50G-4 | 50G-2 | 50G}
```

**100G-2** the default VEP mode. Multiple session bandwidth limited to 200Gbps. Single session bandwidth limited to 100Gbps.

**100G** both multiple session and single-session bandwidth limited to 100Gbps.

**50G-4** multiple session bandwidth limited to 200Gbps. Single session bandwidth limited to 50Gbps.

**50G-2** multiple session bandwidth limited to 100Gbps. Single session bandwidth limited to 50Gbps.

**50G** multiple session bandwidth limited to 50Gbps. Single session bandwidth limited to 50Gbps.

After using this command to select a VEP mode, you must manually restart the FortiGate for the new VEP mode to take affect.

The VEP mode is applied per NP7 processor. If your FortiGate has multiple NP7 processors, they will all operate in the same VEP mode.

## Controlling the maximum outgoing VLAN bandwidth

When configuring a VLAN interface, you can use the new `outbandwidth` option to set the maximum outgoing bandwidth that traffic over the VLAN interface can use.

```
config system interface
  edit "vlan11-vdom1"
    set vdom "vdom1"
    ...
    set outbandwidth <max-bandwidth>
    ...
```

```
set interface "npu0_vlink0"  
set vlanid 11  
end
```

<max-bandwidth> set the maximum outgoing bandwidth in kbps for the VLAN interface. The default is 0 which means no maximum. The range is 0 to 100000000 kbps.

Controlling outgoing VLAN bandwidth can be useful for limiting the amount of bandwidth used by a VLAN interface added to an NPU accelerated VDOM link interface. The NP7 virtual egress processor (VEP) controls the amount of bandwidth that can be used by NPU accelerated VDOM link interfaces. If you are experiencing VEP oversubscription issues due to the amount of traffic passing through VLAN interfaces added to NPU accelerated VDOM link interfaces, you can use the VLAN interface `outbandwidth` option to control the amount of traffic that can pass through the VLAN interface. For more information about VEP, see [Bandwidth control for NPU accelerated VDOM link interfaces on page 11](#).

## Distribute HA session synchronization packets to multiple CPUs

FortiGates with NP7 processors now support using the following command to synchronize HA session sync packets to multiple CPUs:

```
config system ha  
set sync-packet-balance {disable | enable}  
end
```

The `sync-packet-balance` option has the same results when enabled on FortiGates with NP7 processors and NP6 processors.

## SNMP improvements

FortiOS 6.2.7 includes the following SNMP improvements.

### SNMP queries for hardware session counts

You can use the following MIB fields to send SNMP queries for NP7 IPv4 and IPv6 hardware session counts and session setup rates.

The session rate information depends on the hardware logging configuration:

- If hardware logging is set to use the NP7 processors for logging, the IPv4 and IPv6 session counts and session setup rates will both be a total of the IPv4 and IPv6 rates and appear to be the same in SNMP queries.
- If hardware logging is set to use the FortiGate CPUs the IPv4 and IPv6 rates will be correct.

**Path:** FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgSystem.fgSystemInfo

**OID:** 1.3.6.1.4.1.12356.101.4.1

Index	MIB field	Description
.23	fgSysNpuSesCount	NP7 IPv4 session count.
.24	fgSysNpuSesRate1	NP7 IPv4 session setup rate in the last 1 minute.
.25	fgSysNpuSesRate10	NP7 IPv4 session setup rate in the last 10 minutes.
.26	fgSysNpuSesRate30	NP7 IPv4 session setup rate in the last 30 minutes.
.27	fgSysNpuSesRate60	NP7 IPv4 session setup rate in the last 60 minutes.
.28	fgSysNpuSes6Count	NP7 IPv6 session count.
.29	fgSysNpuSes6Rate1	NP7 IPv6 session setup rate in the last 1 minute.
.30	fgSysNpuSes6Rate10	NP7 IPv6 session setup rate in the last 10 minutes.
.31	fgSysNpuSes6Rate30	NP7 IPv6 session setup rate in the last 30 minutes.
.32	fgSysNpuSes6Rate60	NP7 IPv6 session setup rate in the last 60 minutes.

## SNMP queries for NAT46 and NAT64 policy statistics

You can use the following MIB fields to send SNMP queries for hyperscale firewall NAT46 and NAT64 policy statistics. These MIB fields are available from the latest FORTINET-FORTIGATE-MIB.mib.

**Path:** FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgFirewall.fgFwPolicies.fgFwPolTables

**OID:** 1.3.6.1.4.1.12356.101.5.1.2

Index	MIB field	Description
.5	fgFwHsPol46StatsTable	NAT46 hyperscale firewall policy statistics table.
.5.1	fgFwHsPol46StatsEntry	NAT46 hyperscale firewall policy statistics entry.
.5.1.1	fgFwHsPol46ID	NAT46 hyperscale firewall policy ID.

Index	MIB field	Description
.5.1.2	fgFwHsPol46PktCount	NAT46 hyperscale firewall policy packet count.
.5.1.3	fgFwHsPol46ByteCount	NAT46 hyperscale firewall policy byte count.
.5.1.4	fgFwHsPol46LastUsed	The last date and time the NAT46 hyperscale firewall policy was used to start a session.
.6	fgFwHsPol64StatsTable	NAT64 hyperscale firewall policy statistics table.
.6.1	fgFwHsPol64StatsEntry	NAT64 hyperscale firewall policy statistics entry.
.6.1.1	fgFwHsPol64ID	NAT64 hyperscale firewall policy ID.
.6.1.2	fgFwHsPol64PktCount	NAT64 hyperscale firewall policy packet count.
.6.1.3	fgFwHsPol64ByteCount	NAT64 hyperscale firewall policy byte count.
.6.1.4	fgFwHsPol64LastUsed	The last date and time the NAT64 hyperscale firewall policy was used to start a session.

Queries of these fields follow the convention `.oid.<vdom-id>.<policy-id>`

Example SNMP query for NAT46 hyperscale firewall policy statistics:

```
$ snmpwalk -v2c -c public <ip-address> 1.3.6.1.4.1.12356.101.5.1.2.5.1
```

Example SNMP query for NAT64 hyperscale firewall policy statistics:

```
$ snmpwalk -v2c -c public <ip-address> 1.3.6.1.4.1.12356.101.5.1.2.6.1
```

## SNMP queries of NP7 fgProcessor MIB fields

FortiGates with NP7 processors can now respond to SNMP queries for the following paths and OIDs:

- Path: FORTINET-FORTIGATE-MIB:fgProcessorCount  
OID: 1.3.6.1.4.1.12356.101.4.4.1
- Path: FORTINET-FORTIGATE-MIB:fgProcessorModuleCount  
OID: 1.3.6.1.4.1.12356.101.4.5

For example, for a FortiGate-4200F:

```
root@pc1:~# snmpwalk -v2c -c REGR-SYS 10.1.100.1 1.3.6.1.4.1.12356.101.4.4.1
FORTINET-FORTIGATE-MIB::fgProcessorCount.0 = INTEGER: 84
root@pc1:~# snmpwalk -v2c -c REGR-SYS 10.1.100.1 1.3.6.1.4.1.12356.101.4.5
```

```
FORTINET-FORTIGATE-MIB::fgProcessorModuleCount.0 = INTEGER: 5
FORTINET-FORTIGATE-MIB::fgProcModIndex.1 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fgProcModIndex.2 = INTEGER: 2
FORTINET-FORTIGATE-MIB::fgProcModIndex.3 = INTEGER: 3
FORTINET-FORTIGATE-MIB::fgProcModIndex.4 = INTEGER: 4
FORTINET-FORTIGATE-MIB::fgProcModIndex.5 = INTEGER: 5
FORTINET-FORTIGATE-MIB::fgProcModType.1 = OID: FORTINET-FORTIGATE-MIB::fgProcModIntegrated
FORTINET-FORTIGATE-MIB::fgProcModType.2 = OID: FORTINET-FORTIGATE-MIB::fgProcModFnXE2
FORTINET-FORTIGATE-MIB::fgProcModType.3 = OID: FORTINET-FORTIGATE-MIB::fgProcModFnXE2
FORTINET-FORTIGATE-MIB::fgProcModType.4 = OID: FORTINET-FORTIGATE-MIB::fgProcModFnXE2
FORTINET-FORTIGATE-MIB::fgProcModType.5 = OID: FORTINET-FORTIGATE-MIB::fgProcModFnXE2
FORTINET-FORTIGATE-MIB::fgProcModName.1 = STRING: integrated_cpus
FORTINET-FORTIGATE-MIB::fgProcModName.2 = STRING: Integrated_NPU (np7_0)
FORTINET-FORTIGATE-MIB::fgProcModName.3 = STRING: Integrated_NPU (np7_1)
FORTINET-FORTIGATE-MIB::fgProcModName.4 = STRING: Integrated_NPU (np7_2)
FORTINET-FORTIGATE-MIB::fgProcModName.5 = STRING: Integrated_NPU (np7_3)
FORTINET-FORTIGATE-MIB::fgProcModDescr.1 = STRING: Fortinet integrated CPU module (main CPUs
built into device)
FORTINET-FORTIGATE-MIB::fgProcModDescr.2 = STRING: Fortinet integrated CPU module (NPUs
built into device)
FORTINET-FORTIGATE-MIB::fgProcModDescr.3 = STRING: Fortinet integrated CPU module (NPUs
built into device)
FORTINET-FORTIGATE-MIB::fgProcModDescr.4 = STRING: Fortinet integrated CPU module (NPUs
built into device)
FORTINET-FORTIGATE-MIB::fgProcModDescr.5 = STRING: Fortinet integrated CPU module (NPUs
built into device)
FORTINET-FORTIGATE-MIB::fgProcModProcessorCount.1 = INTEGER: 80
FORTINET-FORTIGATE-MIB::fgProcModProcessorCount.2 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fgProcModProcessorCount.3 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fgProcModProcessorCount.4 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fgProcModProcessorCount.5 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fgProcModMemCapacity.1 = Gauge32: 397046052
FORTINET-FORTIGATE-MIB::fgProcModMemCapacity.2 = Gauge32: 8388608
FORTINET-FORTIGATE-MIB::fgProcModMemCapacity.3 = Gauge32: 8388608
FORTINET-FORTIGATE-MIB::fgProcModMemCapacity.4 = Gauge32: 8388608
FORTINET-FORTIGATE-MIB::fgProcModMemCapacity.5 = Gauge32: 8388608
FORTINET-FORTIGATE-MIB::fgProcModMemUsage.1 = Gauge32: 4
FORTINET-FORTIGATE-MIB::fgProcModMemUsage.2 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModMemUsage.3 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModMemUsage.4 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModMemUsage.5 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSessionCount.1 = Gauge32: 19
FORTINET-FORTIGATE-MIB::fgProcModSessionCount.2 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSessionCount.3 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSessionCount.4 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSessionCount.5 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSACount.1 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSACount.2 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSACount.3 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSACount.4 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fgProcModSACount.5 = Gauge32: 0
```

## Maximum number of hyperscale firewall policies increased

The FortiOS 6.2.7 per-VDOM limit for hyperscale firewall policies has been increased to 2000 for each policy type. There are four types of hyperscale firewall policies: IPv4, IPv6, NAT64, and NAT46.

# Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 6.2.7 Build 7105. The [Special notices](#) described in the [FortiOS 6.2.7 release notes](#) also apply to Hyperscale firewall for FortiOS 6.2.7 Build 7105.

## Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 6.2.7, you should verify that the NP queue priority configuration is either your intended configuration or matches the default configuration shown below. If you are upgrading from a FortiOS version that does not support the NP queue priority feature, the NP queue priority configuration after the firmware upgrade could be empty or incorrect.

The default NP queue priority configuration should result in optimal performance in most cases. An empty or incorrect NP queue priority configuration can affect performance or cause traffic disruptions. In the case of a hyperscale firewall VDOM, an empty NP queue priority configuration could cause BGP flapping or traffic interruptions when a lot of IP traffic and/or non-SYN TCP traffic is sent to the CPU.

Here is the default NP queue priority configuration:

```
config system npu
    config np-queues
        config ethernet-type
            edit "ARP"
                set type 806
                set queue 9
            next
            edit "HA-SESSYNC"
                set type 8892
                set queue 11
            next
            edit "HA-DEF"
                set type 8890
                set queue 11
            next
            edit "HC-DEF"
                set type 8891
                set queue 11
            next
            edit "L2EP-DEF"
                set type 8893
                set queue 11
            next
            edit "LACP"
                set type 8809
                set queue 9
            next
        end
    config ip-protocol
```

```
edit "OSPF"
    set protocol 89
    set queue 11
next
edit "IGMP"
    set protocol 2
    set queue 11
next
edit "ICMP"
    set protocol 1
    set queue 3
next
end
config ip-service
edit "IKE"
    set protocol 17
    set sport 500
    set dport 500
    set queue 11
next
edit "BGP"
    set protocol 6
    set sport 179
    set dport 179
    set queue 9
next
edit "BFD-single-hop"
    set protocol 17
    set sport 3784
    set dport 3784
    set queue 11
next
edit "BFD-multiple-hop"
    set protocol 17
    set sport 4784
    set dport 4784
    set queue 11
next
edit "SLBC-management"
    set protocol 17
    set dport 720
    set queue 11
next
edit "SLBC-1"
    set protocol 17
    set sport 11133
    set dport 11133
    set queue 11
next
edit "SLBC-2"
    set protocol 17
    set sport 65435
    set dport 65435
    set queue 11
end
```

## FortiGates with NP7 processors and NetFlow domain IDs

Each NP7 processor and the FortiGate itself all have different NetFlow domain IDs. When the FortiGate sends NetFlow domain information to the NetFlow server, the information includes the separate domain IDs for the FortiGate CPU and each NP7 processor.

Log messages from the FortiGate CPU and from each NP7 processor contain these domain IDs, allowing the NetFlow server to distinguish between FortiGate CPU traffic and traffic from each NP7 processor.

## HPE limitations

For FortiOS 6.2.7 Build 7105, the host protection engine (HPE) can only be used to limit the total number of packets per host queue, only the following options work:

```
config system npu
    config hpe
        set all-protocol <rate>
        set enable-shaper {disable | enable}
    end
```

`all-protocol <rate>` limit to the total number of packets per host queue. The range is 1000 to 1000000000 pps.

For more information about the `config hpe` command, see [config hpe](#).

You can exempt traffic from HPE rate limiting by setting its queue between 8 and 11 using the following command:

```
config system npu
    config np-queues
```

See [config np-queues](#) for details about setting NP queues.

## Hyperscale firewall 6.2.7 incompatibilities and limitations

Hyperscale firewall for FortiOS 6.2.7 has the following limitations and incompatibilities with FortiOS features:

- Proxy or flow based inspection is not supported. You cannot include security profiles in hyperscale firewall policies.
- Single-sign-on authentication including FSSO and RSSO is not supported. Other types of authentication are supported.
- IPsec VPN is not supported. You cannot create hyperscale firewall policies where one of the interfaces is an IPsec VPN interface.
- Hyperscale firewall VDOMs do not support Central NAT.
- Hyperscale firewall VDOMs do not support profile-based NGFW firewall policies.
- Hyperscale firewall VDOMs do not support consolidated firewall policies.
- Hyperscale firewall VDOMs must be NAT mode VDOMs. Hyperscale firewall features are not supported for transparent mode VDOMs.
- Hyperscale firewall VDOMs do not support traffic shaping policies or profiles. Only outbandwidth traffic shaping is supported for hyperscale firewall VDOMs.

- Traffic shaping with queuing using the NP7 QTM module is not compatible with carrier-grade NAT and hyperscale firewall features. See [NP7 traffic shaping](#).
- The proxy action is not supported for DoS policy anomalies in hyperscale firewall VDOMs.
- Active-Active FGCP HA and FGSP do not support HA hardware session synchronization. Active-passive FGCP HA and virtual clustering do support FGCP HA hardware session synchronization.
- Asymmetric sessions are not supported.
- ECMP usage-based load balancing is not supported. Traffic is not directed to routes with lower spillover-thresholds.
- The Sessions dashboard widget does not display hyperscale firewall sessions.
- Interface device identification should not be enabled on interfaces that send or receive hyperscale firewall traffic.
- The `proxy` action is not supported for DoS policy anomalies when your FortiGate is licensed for hyperscale firewall features. When you activate a hyperscale firewall license, the `proxy` option is removed from the CLI of both hyperscale VDOMs and normal VDOMs.
- During normal operation, UDP sessions from protocols that use FortiOS session helpers are processed by the CPU. After an FGCP HA failover, when the UDP session helper sessions are re-established, they will not be identified as session helper sessions and instead will be offloaded to the NP7 processors.
- When operating an FGCP HA cluster with session synchronization enabled, some of the sessions accepted by an IPv4 or a NAT64 hyperscale firewall policy with an overload IP pool may not be synchronized to the secondary FortiGate. Some sessions are not synchronized because of resource conflicts and retries. The session loss rate depends on the percentage of resource retries during session setup. You can reduce the session loss by making sure the IP pool has as many IP addresses and ports as possible.
- The following options are not supported for IPv4 firewall VIPs (configured with the `config firewall vip` command) in hyperscale firewall VDOMs: `src-filter`, `service`, `nat44`, `nat46`, `nat-source-vip`, `arp-reply`, `portforward`, and `srcintf-filter`.
- The following options are not supported for port forwarding IPv6 firewall VIPs (configured with the `config firewall vip6` command) in hyperscale firewall VDOMs: `src-filter`, `nat-source-vip`, `arp-reply`, `portforward`, `nat66`, and `nat64`.



Even though the `arp-reply` CLI option is not supported for IPv4 and IPv6 firewall VIPs, responding to ARP requests for IP addresses in a virtual IP is supported. What is not supported is using the `arp-reply` option to disable responding to an ARP request.

## About hairpinning

You can use Endpoint Independent Filtering (EIF) to support hairpinning. A hairpinning configuration allows a client to communicate with a server that is on the same network as the client, but the communication takes place through the FortiGate because the client only knows the external address of the server.

To set up a hyperscale firewall hairpinning configuration, you need to enable EIF in the hyperscale firewall policy. As well, the IP pool added to the policy should include addresses that overlap with the firewall policy destination address. In many cases you can do this by setting the firewall policy destination address to all.

If the policy uses a specific address or address range for the destination address, then this destination address and the IP pool address range should have some overlap.

## **Interface device identification is not compatible with hyperscale firewall traffic**

Device identification should be disabled on interfaces that receive or send hyperscale firewall traffic. Device identification is usually disabled by default for physical interfaces. However, if you add a new interface, for example to create a VLAN or a LAG, device identification may be enabled by default and if so, should be disabled.

# Upgrade information

Refer to the Upgrade Path Tool (<https://docs.fortinet.com/upgrade-tool>) in the Fortinet documentation library to find supported upgrade paths for all FortiGate models and firmware versions.

A similar upgrade path tool is also available from Fortinet Support: <https://support.fortinet.com>.

See also, [Upgrade information](#) in the [FortiOS 6.2.7 release notes](#).

In some cases, these upgrade path tools may recommend slightly different upgrade paths. If that occurs, the paths provided by both tools are supported and you can use either one.



After the firmware upgrade is complete, you should check the NP queue priority configuration. In some cases the NP queue priority configuration may be incorrect after a firmware upgrade. For more information, see [Check the NP queue priority configuration after a firmware upgrade on page 17](#).

---

If your FortiGate is currently running FortiOS 6.2.6 firmware and is licensed for hyperscale firewall features, you can follow a normal firmware upgrade process to upgrade to FortiOS 6.2.7.

If you are currently operating a FortiGate-4200F, 4201F, 4400F, or 4401F with an older firmware version than 6.2.6 and a hyperscale firewall license, you can upgrade in one step to FortiOS 6.2.7 because upgrading to FortiOS 6.2.7 will remove the existing hyperscale firewall configuration but the hyperscale firewall license will still be active. You can go ahead and create a new hyperscale firewall configuration for FortiOS 6.2.7.

If you are currently operating a FortiGate-4200F, 4201F, 4400F, or 4401F without a hyperscale firewall license you can use the upgrade path to upgrade to FortiOS 6.2.7. To configure hyperscale firewall features, activate your hyperscale firewall license and set up the hyperscale firewall configuration.



The FortiOS 6.2.7 hyperscale firewall configuration is very different from the 6.2.5 configuration. Upgrading a FortiGate-4200F, 4201F, 4400F, or 4401F from FortiOS 6.2.5 to 6.2.7 will require significant time for preparation and planning before the firmware upgrade and significant downtime after the firmware upgrade to create the new configuration.

---

## To upgrade an HA cluster from an older firmware version

Recommended procedure for upgrading an HA cluster from FortiOS 6.2.5 and older to FortiOS 6.2.7:

1. Disconnect the backup FortiGate from the cluster.
2. Upgrade the backup FortiGate's firmware to FortiOS 6.2.7 and set the configuration to factory defaults.
3. Create the new FortiOS 6.2.7 hyperscale firewall configuration on the backup FortiGate.  
Fortinet Support can assist with setting up the new configuration.
4. When the backup FortiGate is reconfigured and the configuration tested you can swap network connections from the primary FortiGate to the backup FortiGate with minimal downtime.
5. Then you can upgrade the firmware on the primary FortiGate and reset it to factory defaults.
6. Apply the new hyperscale configuration to the primary FortiGate.

Do this before reforming the cluster, since some configurations may require restarting the FortiGate.

7. Add the primary FortiGate back to the cluster to re-form the cluster.

## To upgrade a standalone FortiGate from an older firmware version

To upgrade a standalone FortiGate from FortiOS 6.2.5 and older to FortiOS 6.2.7, Fortinet recommends preparing the new configuration on a test device if possible before configuring your production FortiGate. Fortinet Support can help with planning, configuration, and conversion.

# Product integration and support

This section describes Hyperscale firewall for FortiOS 6.2.7 Build 7105 product integration and support information. The [Product integration and support](#) information described in the [FortiOS 6.2.7 release notes](#) also applies to Hyperscale firewall for FortiOS 6.2.7 Build 7105.

Hyperscale firewall for FortiOS 6.2.7 Build 7105 requires the following or newer versions of FortiManager and FortiAnalyzer:

- FortiManager 6.2.8 ([FortiManager 6.2.8 Release Notes](#)) or 6.4.6 ([FortiManager 6.4.6 Release Notes](#))
- FortiAnalyzer 6.2.8 ([FortiAnalyzer 6.2.8 Release Notes](#)) or 6.4.6 ([FortiAnalyzer 6.4.6 Release Notes](#))

## Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 6.2.7 are available from the FortiOS Maximum Values Table (<https://docs.fortinet.com/max-value-table>).

# Resolved issues

The following issues have been fixed in Hyperscale firewall for FortiOS 6.2.7 Build 7105. For inquiries about a particular bug, please contact [Customer Service & Support](#). The [Resolved issues](#) described in the [FortiOS 6.2.7 release notes](#) also apply to Hyperscale firewall for FortiOS 6.2.7 Build 7105.

Bug ID	Description
643446	Fragmented packets with different Explicit Congestion Notification (ECN) values are now allowed. Not allowing fragmented packets with different ECN values had resulted in some customers experiencing dropped packets.
665669	SFP28 and QSFP28 interfaces in FortiGates with NP7 processors now support Clause 74 forward error correction (FEC).
676525	Sessions are no longer lost if a policy route is deleted or an interface is shut down.
0678390	The <code>get system ha status</code> command displays information about the total number of hardware session-sync sessions.
684052	The implicit deny policy can now appear on the GUI in hyperscale firewall policy lists.
685992	Improved dependency checking when adding or editing GCN IP pools and hyperscale firewall policies.
686774	FortiGate-1800F and 1801F sensor data now appears as expected on the GUI and CLI.
687034	Resolved a BGP memory leak.
687749	Resolved an issue that caused the <code>iked</code> process to crash on the secondary FortiGate in an FGCP HA cluster for IPsec VPN tunnels using XAUTH authentication.
687990	Hyperscale firewall systems can now generate system event log messages to report on network processor daemon (NPD) and PLE errors that would otherwise just have been written to the console. Example log message: <code>date=2021-04-28 time=22:18:40 logid="0100053300" type="event" subtype="system" level="warning" vd="root" eventtime=1619673521069002897 tz="-0700" logdesc="NPD INFO" msg=" NPD INIT DONE "</code>
688309	Resolved an issue that caused packets to randomly be dropped when passing through NPU accelerated VDOM link interfaces.
689660	Policy hit counters have been implemented for hyperscale firewall policies.
690469	The Sessions dashboard will no longer revert to 3 x 1 after being re-sized.
691166	The <code>diagnose sys npu-session purge</code> command now successfully purges all session data.
692241	BGP no longer consumes high amounts of CPU time when an ADVPN disconnects after a socket writing error.
692737	Resolved an issue that caused timeout errors on the secondary FortiGate in an FGCP cluster when a fixed allocation IP pool was changed to an overload IP pool.

Bug ID	Description
694645	Resolved an issue that blocked NAT64 traffic when a hyperscale firewall policy included an IPv6 firewall virtual IP.
694747	Error messages no longer appear on the CLI console when setting VDOM mode to <code>no-vdom</code> .
695262	In a hyperscale firewall policy, you can no longer incorrectly select Negate after setting the service to All.
695732	You can now create a cluster of two FortiGates with different interface configurations. If you do this, the secondary FortiGate will be re-configured to match the configuration of the primary FortiGate. However, it is still recommended that both FortiGates have the same interface configuration before creating a cluster.
696133	Policy routing works as expected.
696236	Resolved an issue that can cause BGP flapping.
698587	When configuring a Hyperscale firewall SPU offload logging from the GUI you can set the logging mode of a log server group to Per-Session ending.
698677	If you restore a configuration and the configuration file contains a VDOM with the policy offload level set to full-offload but with a VDOM name that doesn't following the hyperscale firewall VDOM naming convention, the policy offload level will be set to disable when the configuration is restored.
698834	Resolved an issue that resulted in malformed log message packets.
699162	Resolved an issue that blocked administrative access to a transparent mode VDOM when connecting to an interface in the VDOM.
699236 701715	Resolved an issue that could cause the NPD to hang and result in PBA leaks.
699348	MTU settings for VLAN interfaces are now kept after a system restart.
699348	MTU size settings are no longer lost for VLAN interfaces after a system restart.
700158	Resolved an issue that could cause a kernel panic when creating an EMAC VLAN.
700271	In an active-passive FCGP cluster of two FortiGates licensed for hyperscale firewall features, the secondary FortiGate in the cluster no longer responds to ARP requests.
700479	Resolved an issue that in some cases caused the Sessions dashboard widget to show more sessions than what the system was actually processing.
701228	The <code>diagnose npu np7 gtp-stats-all</code> command no longer requires an NPU ID.
704140	Improved the accuracy of the SPU statistics displayed on the GUI.
704328	The interface used for HA hardware session synchronization can no longer incorrectly be assigned an IP address.
704463	Resolved a VXLAN throughput performance issue.
704741	The execute disk scan command now works as expected on systems with log disks.
705118	Resolved multiple NP7-related DoS protection bugs.
705322	Resolved an issue that could block session synchronization between FGSP peers.

Bug ID	Description
705329	FortiGates with NP7 processors now support using a LAG interface for FGSP session synchronization.
705792 708569	Resolved multiple issue with NP7 CAPWAP offloading that could block client traffic when the <code>dtls-policy</code> setting on the FortiAP device is set to clear text or IPsec VPN.
705902	Resolved an issue that caused a PBA leak while running a high amount of UDP traffic.
706150	Resolved an issue with EIF and ALG session handling that can cause sessions to be lost and problems with resource allocation.
706196 709892	Resolved syntax check issues that prevented adding valid policy routes that do not have a gateway configured and allowed adding invalid policy routes with no outgoing interface configured.
706256	Any valid address object, including an FQDN address, can be added to a DoS policy.
706601	Resolved an issue that caused the output of the <code>diagnose sys npu-session list</code> command to show the wrong duration time for sessions on a secondary FortiGate in an FGCP cluster.
706871	Improved the quality of the information displayed by the <code>diagnose npd policy sync</code> command.
707714 703290 709590 709786	Various NPD process crash issues.
708415	The <code>per-session-ending</code> log mode now works as expected if the FortiGate is set to use the CPU for hardware logging. See <a href="#">Configuring hardware logging</a> for more information.
708839	Resolved an issue that could cause a FortiGate with CAPWAP offloading to become unresponsive when adding a VLAN interface to a wireless interface.
708874	Resolved an issue that could cause delays for some types of traffic after an HA failover.
709046	Resolved an issue that could cause inaccurate statistics reporting when the system is processing a large number of sessions.
709481	Added support for proxy-based SIP in hyperscale firewall VDOMs.
710219	Added support for VLANs over LAG for GTPu enhanced mode traffic.
710232	Resolved an issue that caused BGP flapping when processing high levels of bursty traffic or when processing fragmented packets.
710475 709091	The <code>diagnose sys npu-session stats</code> command now displays the correct IPv6 session setup rate.
710748	Resolved an issue that could prevent QSFP28 interfaces from connecting when speed is set to <code>40000full</code> .
710999	The <code>config dsw-dts-profile</code> option of the <code>config system npu</code> command is now available for the FortiGate-4200F/4201F/4400F/4401F. See <a href="#">config dsw-dts-profile</a> .
712291	Forward error correction (FEC) is now set correctly for split interfaces.
712517	Resolved multiple issues that could prevent NAT64 hairpin policies from working as expected.

Bug ID	Description
713821	Information displayed by the <code>diagnose firewall iprop6 show</code> command is now correct.
714342	The <code>diagnose hardware deviceinfo nic</code> command no longer shows extra interfaces.
714350	Resolved an issue that could cause the VLAN ID to be missing from exception packets to and from VLAN interfaces.
725268	IPsec traffic can now be offloaded when being sent over an EMAC VLAN interface.

# Known issues

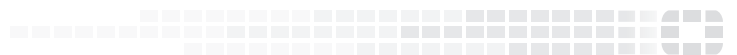
The following issues have been identified in Hyperscale firewall for FortiOS 6.2.7 Build 7105. For inquiries about a particular bug, please contact [Customer Service & Support](#). The [Known issues](#) described in the [FortiOS 6.2.7 release notes](#) also apply to Hyperscale firewall for FortiOS 6.2.7 Build 7105.

Bug ID	Description
669645	VXLAN interfaces cannot be added to a hardware switch interface.
678318	Apply NP7 acceleration to inter-VDOM link traffic by creating inter-VDOM links with the <code>type</code> set to <code>npupair</code> . For example: <pre>config system vdom-link   edit &lt;name&gt;     set type npupair   end</pre>
692021	Only one hardware session synch interface can be configured in an HA configuration.
701987	The NP7 hyperscale firewall packet sniffer ( <code>diagnose npu sniffer</code> ) does not work for IPv4 or IPv6 VPN tunnel interfaces.
703667	FGCP HA hardware session synchronization may not synchronize all hyperscale firewall sessions to the backup FortiGate if the hyperscale firewall session includes one or more overload IP pools. The session loss rate on the backup FortiGate depends on the percentage of resource retries during session setup. The more IP pool resources that are available, the lower the loss rate.
704851	The <code>config system session-ttl</code> command is a VDOM command, configured from a VDOM. However, options set by this command apply to all CGNAT VDOMs and not just the VDOM in which they are set.
706696	SNMP UDP traffic passing through a FortiGate is intimidatingly dropped when NP7 hardware acceleration is enabled .
707729	In some cases a temporary performance reduction occurs when changing the firewall configuration or running some <code>diagnose</code> commands on a FortiGate under high traffic load.
709110	During startup, there may be a delay as various processes start up before sessions can be sent to the NP7 processors. Sessions received during this delay that would normally be NP7 sessions may be processed by the CPU.
709890	In some cases, SIP data sessions may be unexpectedly offloaded to NP7 processors.
710083	If the <code>udp-idle-timer</code> is set to a relatively high value, a FortiGate may enter into conserve mode from running lower than expected amounts of SIP traffic.
710232	HPE functionality is limited in this release. For details, see <a href="#">HPE limitations on page 19</a> .
711135	Various HA-related issues can cause minor performance reductions or unexpected behavior.
711462	
714800	
716766	

Bug ID	Description
718059	
714915	Changing the configuration of a hardware log server group assigned to a hyperscale firewall policy that is processing traffic may cause sessions accepted by the firewall policy to be dropped.
715532	Due to an index limit, a FortiGate may not be able to manage a FortiSwitch if the FortiGate is licensed for 500 VDOMs and you have created a large number of VDOMs (for example, over 300).
716169	SPF interfaces with speed set to 1000full will remain down after the system restarts.
716245	In the hyperscale firewall policy list, the GUI does not accurately display the number of bytes or packets processed by the explicit deny policy.
716424	The NPD process crashes if a FortiGate is under relatively high traffic load and the configuration includes the maximum number of hyperscale firewall policies, as defined in the maximum values, in multiple VDOMs.
717011	In some cases, SIP ALG traffic can cause PBA leaks and deadlocks.
717071	While editing a hyperscale firewall policy, if you edit the IP pool configuration added to the policy and enable overload, the Endpoint Independent Mapping option in the firewall policy incorrectly remains visible. Endpoint Independent Mapping is not supported for hyperscale firewall policies with overload IP pools.
717304	Time displayed by the real time clock may drift and become inaccurate. You can work around this issue by enabling NTP.
717621	In some cases, in a FortiGate with multiple NP7s one of the NP7 processors can appear to be much busier than the others.
718356	In some cases, BGP prefixes are not cleared from the routing table used by NP7 processors after they have been removed from the kernel because the peer they point to has gone down.
718373	It may take more time than expected to install BGP prefixes in the routing table used by NP7 processors. During the delay the GUI and CLI may not be accessible.
718429	SIP RTCP sessions accepted by hyperscale firewall policies may not be offloaded to NP7 processors.
718442	SNMP queries for NAT64 session counts may not return any data.
718713	An interface that is configured to drop fragmented packets ( <code>drop-fragment</code> set to <code>enable</code> ) may still forward fragmented packets.
718886	In some cases, when the SIP session helper is enabled, some SIP traffic is offloaded to NP7 processors. SIP traffic should not be offloaded if the SIP session helper is enabled.
725975	Hyperscale firewall policy usage statistics are not displayed on the GUI when editing the policy.
740225	In hyperscale VDOMs, traffic may be blocked by NP7 processors if the firewall policy that accepts the traffic includes address groups with ten or more firewall addresses if one or more of the firewall addresses in the address group matches a single IP address. You can work around this problem by removing the firewall addresses from the address group that match a single IP address and adding these firewall addresses directly to the firewall policy. After making the configuration change, you should restart the FortiGate.



**FORTINET®**



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.