Hyperscale Firewall - Release Notes

Version 6.4.8 Build 6165

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

January 11, 2023
Hyperscale Firewall 6.4.8 Build 6165 Release Notes
01-648-754335-20230111

TABLE OF CONTENTS

Change log

Date	Change description
January 11, 2023	Added more information about `arp-reply` support limitations for IPv4 and IPv6 firewall VIPs to Hyperscale firewall 6.4.8 incompatibilities and limitations on page 14.
April 29, 2022	Added information to Upgrade information on page 17 about confirming the configuration of the `dsw-queue-dts-profile` option of the `config system npu` command after upgrading to FortiOS 6.4.8.
February 14, 2022	New section: Check the NP queue priority configuration after a firmware upgrade on page 12. Also, a note has been added about this issue to, Upgrade information on page 17.
December 2, 2021	Improved the information in Changes to setting the hyperscale VDOM policy offload level on page 6. Added two new FGCP HA-related limitations to Hyperscale firewall 6.4.8 incompatibilities and limitations on page 14.
November 25, 2021	Misc. fixes.
November 24, 2021	Initial version.

Hyperscale firewall for FortiOS 6.4.8 release notes

These platform specific release notes describe new features, changes in table size, special notices, upgrade information, product integration and support, resolved issues, and known issues for FortGates licensed for Hyperscale firewall features for FortiOS 6.4.8 Build 6165.

In addition, special notices, changes in the CLI, changes in default behavior, changes in table size, new features and enhancements, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 6.4.8 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 6.4.8 Build 6165.

For Hyperscale firewall documentation for this release, see the Hyperscale Firewall Guide.

For NP7 hardware acceleration documentation for this release, see the Hardware Acceleration Guide.

Supported FortiGate models

Hyperscale firewall for FortiOS 6.4.8 Build 6165 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 6.4.8 Build 6165.

Changes to setting the hyperscale VDOM policy offload level

FortiOS 6.4.8 includes the following command to change the policy offload level of a hyperscale firewall VDOM:

```
config system setings
   set policy-offload-level {disable | dos-offload | full-offload}
end
```

`disable` disable hyperscale firewall features and disable offloading DoS policy sessions to NP7 processors for this VDOM. All sessions are initiated by the CPU. Sessions that can be offloaded are sent to NP7 processors. This is the default setting.

`dos-offload` offload DoS policy sessions to NP7 processors for this VDOM. All other sessions are initiated by the CPU. Sessions that can be offloaded are sent to NP7 processors.

`full-offload` enable hyperscale firewall features for the current hyperscale firewall VDOM. This option is only available if the FortiGate is licensed for hyperscale firewall features. DoS policy sessions are also offloaded to NP7 processors. All other sessions are initiated by the CPU. Sessions that can be offloaded are sent to NP7 processors.

FortiOS 6.4.8 removes the `default` option of the `policy-offload-level` command that was available for previous versions. When upgrading from a previous version of FortiOS to version 6.4.8, if `policy-offload-level` is set to `default` before the upgrade, the firmware upgrade process changes the setting to `disable`.

Allowing packet fragments for NP7 NAT46 policies when the DF bit is set to 1

The packet size increase that occurs when a NAT46 hyperscale firewall policy converts an IPv4 packet into an IPv6 packet can cause the packet to be dropped if the larger packet exceeds the outgoing interface MTU and the DF bit is set to 1 (do not fragment). You can use the following command to cause NP7 processors to override the DF setting and fragment and forward the packet instead of dropping it. This is a global setting that affects all NAT64 traffic offloaded by NP7 processors.

```
config system npu
   set nat46-force-ipv4-packet-forwarding enable
end
```

When this option is disabled, packets with DF=1 that exceed the outgoing interface MTU are dropped.

Prevent CPU or host logging packet loss

In some cases, hyperscale firewall CPU or host logging packets can be dropped, resulting in lost log messages and incorrect traffic statistics. You can use the following command to change how your FortiGate queues CPU or host logging packets.

```
config log npu-server
   set log-processor host
   set log-processing {may-drop | no-drop}
end
```

`may-drop` the default CPU or host log queuing method is used. Log message packet loss can occur if the FortiGate is very busy.

`no-drop` use an alternate queuing method that prevents packet loss.

NP7 handling of ICMP checksum errors during anomaly checking

You can use the following command to configure NP7 processors to send ICMP packets with checksum errors to the CPU:

```
config system npu
   config fp-anomaly
      set icmp-csum-err trap-to-host
   end
```

You might set up this configuration if you have configured a DoS firewall policy that includes ICMP DoS protection.

In addition to the above configuration, you must also use the following command (new to FortiOS 6.4.8) to block or allow NP7 processors to send ICMP packets with checksum errors to the CPU:

```
config system npu
   set htx-icmp-csum-chk {drop | pass}
end
```

`drop` block ICMP packets with checksum errors. This is the default setting.

`pass` forward ICMP packets with checksum errors to the CPU.

Configuring background SSE scanning

To support reporting accurate UDP session statistics, normal UDP session synchronization is disabled for FortiGates with hyperscale firewall features enabled and background Session Search Engine (SSE) scanning is used to keep UDP sessions synchronized.

Background SSE scanning uses the CPU instead of the NP7 processors and can cause CPU spikes; however, these spikes should not usually affect overall performance. You can use the following command to adjust background SSE scanning behavior:

```
config system npu
   config background-sse-scan
      set scan {disable | enable}
```

```
    set stats-update-interval <interval>
    set udp-keepalive-interval <interval>
end
```

`scan` enable or disable background SSE scanning. This option is enabled by default. If disabled, UDP O-session and R-session synchronization is enabled so UDP sessions will remain synchronized. However, the statistics reported by traffic logging for UDP O-sessions will be incorrect.

`stats-update-interval` statistics update interval in seconds. The range is 300 to 1073741823 seconds and the default update interval is 300 seconds. You can increase the statistics update interval to reduce how often the CPU is used for SSE background scanning.

`udp-keepalive-interval` UDP keepalive interval in seconds. The range is 90 to 1073741823 seconds and the default keepalive interval is 90 seconds. The 90 second keepalive interval is recommended because the default UDP session timeout is 180 seconds. If you increase the keepalive interval, some UDP sessions may be dropped prematurely.

Hyperscale firewall VDOM asymmetric routing with ECMP support

Hyperscale firewall VDOMs for FortiOS 6.4.8 have improved support for asymmetric routing and ECMP. In most cases asymmetric routing will work the same way in a hyperscale firewall VDOM as in a normal VDOM, with the following notes and exceptions:

- The `auxiliary-session` and `asymroute-icmp` options of the `config system settings` command do not have to be enabled for the hyperscale firewall VDOM for asymmetric routing to work.
- Make sure that original routes (O-routes) do not overlap with reverse routes (R-routes). If you have created overlapping O- and R-routes, all reply traffic uses the same O-route.
- If possible, create an even number of ECMP paths. Traffic distribution is uneven if you have an odd number of ECMP paths. For example, if your configuration includes one O-route and three R-routes, the reply traffic distribution will be approximately 2:1:1 among the three R-routes.

Adjusting NP7 hyperscale firewall blackhole and loopback route behavior

You can use the following diagnose command to configure how the NP7 hyperscale firewall policy engine handles traffic in a hyperscale firewall VDOM that matches a blackhole route or a loopback route. The NP7 policy engine is implemented by the NP7 `npd` process. By default the NP7 policy engine:

- Drops traffic that matches a blackhole route (drop).
- Sends traffic that matches a loopback route to the CPU (host).

You can use the following diagnose command to change this behavior. Because this is a diagnose command, any changes are reverted to defaults when the FortiGate restarts:

The command syntax is:

```
diagnose npd debug cmd 14 {28 | 29} {0 | 1 | 2}
```

`28` configure how the NP7 policy engine handles traffic that matches a blackhole route.

`29` configure how the NP7 policy engine handles traffic that matches a loopback route.

`0` set blackhole or loopback route handling to ignore.

`1` send traffic that matches a blackhole or loopback route to the CPU (host).

`2` drop traffic that matches a blackhole or loopback route.

For example, use the following command to send traffic that matches a blackhole route to the CPU:

```
diagnose npd debug cmd 14 28 1
```

Use the following command to set loopback routing to drop:

```
diagnose npd debug cmd 14 29 2
```

Viewing the NP7 hyperscale policy engine routing configuration

You can use the following diagnose command to view the current NP7 hyperscale policy engine routing configuration. You can also use this command to add and remove routes. Because this is a diagnose command, any changes are reverted to defaults when the FortiGate restarts:

```
diagnose npd route {lookup | dump | stats| sync | flush | add | del}
```

`lookup` lookup route links.

`dump` list the NP7 policy engine routing table.

`stats` display route statistics.

`sync` update the NP7 policy engine routing table to match the CPU kernel routing table.

`flush` flush the NP7 policy engine routing table.

`add` add a route to the NP7 policy engine routing table.

`del` delete a route to the NP7 policy engine routing table.

The syntax for the `add` and `del` command is:

```
diagnose npd route {add | del} <destination> <prefix-length> <gateway> <oif> <table> <scope>
     <type> <proto> <priority> <tos> <flags>
```

For blackhole and loopback routes, set `<flags>` to the following nh_flags values:

- For blackhole routes the nh_flags value is 0x80.
- For loopback routes, the nh_flags value is 0x100.

For example, use the following command to add a blackhole route to the NP7 policy engine routing table:

```
diagnose npd route add 1.1.1.1 24 0.0.0.0 54 254 0 1 11 3333 0 0x80
```

The following command will delete this route from the NP7 policy engine routing table:

```
diagnose npd route del 1.1.1.1 24 0.0.0.0 54 254 0 1 11 3333 0 0x80
```

Enabling or disabling per-policy accounting for hyperscale firewall traffic

Per-policy accounting for hyperscale firewall traffic was added to hyperscale firewall for FortiOS 6.2.7. This change was documented as resolved issue 689660 (Policy hit counters have been implemented for hyperscale firewall policies), in the Resolved issues section of the FortiOS 6.2.7 hyperscale firewall release notes. Per-policy accounting was added to be able to record hit counts for packets accepted or denied by hyperscale firewall policies.

To implement per-policy accounting for hyperscale firewall policies, changes were made to NP7 session management. As a result of these changes, per-policy accounting for hyperscale firewall policies can reduce hyperscale firewall performance.

Hyperscale firewall for FortiOS 6.4.8 includes the following command that you can use to enable or disable hyperscale firewall per-policy accounting for all hyperscale traffic:

```
config system npu
   set per-policy-accounting {disable | enable}
end
```

Per-policy accounting is disabled by default. When per-policy accounting is enabled, you can see hyperscale firewall policy hit counts on the GUI and CLI. If you disable per-policy-accouting for hyperscale firewall traffic, FortiOS will not collect hit count information for traffic accepted or denied by hyperscale firewall policies.

Enabling or disabling per-policy accounting deletes all current sessions, disrupting traffic. Changing the per-policy accounting configuration should only be done during a quiet period.

Displaying more information about NP7 hyperscale firewall hardware sessions

You can use the following diagnose commands to display the current NP7 hyperscale firewall hardware IPv4 and IPv6 session lists:

```
diagnose sys npu-session list
diagnose sys npu-session list6
```

These commands display the current session list stored in the logging buffer. For sessions accepted by firewall policies that use hardware logging (`log-processor` is set to `hardware`), the logging buffer includes all session details. For sessions accepted by firewall policies using CPU or host logging (`log-processor` is set to `host`), the command displays fewer details about the session list, because CPU or host logging only maintains a subset of all of the information available for each session in the session list.

New for FortiOS 6.4.8, you can use the following commands to display the current NP7 hyperscale firewall hardware session list by sending a query to the NP7 Session Search Engine (SSE). The output of these commands does not depend on the hardware logging configuration because they query the SSE. However, because the commands are querying the SSE, the response time will be longer.

```
diagnose sys npu-session list-full
diagnose sys npu-session list-full6
```

Changes in table size

The following changes have been made to table size settings in Hyperscale firewall for FortiOS 6.4.8 Build 6165.

Bug ID	Description
752891 752418	The global firewall.policy limit for the FortiGate-4400F, 4401F, 4200F, and 4201F is increased to 400,000.
737628	The `router.multicast6:interface` table size entry is now unlimited, matching `router.multicast:interface`.

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 6.4.8 Build 6165. The Special notices described in the FortiOS 6.4.8 release notes also apply to Hyperscale firewall for FortiOS 6.4.8 Build 6165.

Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 6.4.8, 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
```

Blackhole and loopback routes and BGP in a hyperscale VDOM

Fortinet recommends that you should not configure hyperscale VDOMs to use blackhole and loopback routes for BGP. By default, blackhole routes are set to drop and loopback routes are set to fwd to CPU and these settings should not be changed.

Forward error correction only available for 100 GigE interfaces

On FortiGate models with NP7 processors, the `forward-error-correction` CLI option is only available for interfaces with speed set to `100Gfull`. Forward error connection is not supported for interfaces in FortiGates with NP7 processors operating at any other speeds.

The following FortiGate models with NP7 processors have 100 GigE interfaces:

- The port17 to port24 interfaces of the FortiGate-4200F and 4201F.
- The port17 to port28 interfaces of the FortiGate-4400F and 4401F.

When the speed of these interfaces set to `40000full`, the `forward-error-correction` CLI option is no longer available.

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.

Hyperscale firewall 6.4.8 incompatibilities and limitations

Hyperscale firewall for FortiOS 6.4.8 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.
- Hyperscale firewall VDOMs do not support traffic that requires session helpers or ALGs (for example, FTP, TFTP, SIP, MGCP, H.323, PPTP, L2TP, ICMP Error/IP-options, PMAP, TNS, DCE-RPC, RAS, and RSH).
- Active-Active FGCP HA and FGSP HA do not support HA hardware session synchronization. Active-passive 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 6.4.8 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.

If your FortiGate is currently running FortiOS 6.2.6, 6.2.7, 6.2.9, or 6.4.6 firmware and is licensed for hyperscale firewall features, you can follow a normal firmware upgrade process to upgrade to FortiOS 6.4.8.

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 6.4.8. Once you have upgraded to 6.4.8 you can activate your hyperscale firewall license and set up your hyperscale firewall configuration.

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 12.

After the firmware upgrade is complete, you should also check the following configuration.

```
config system npu
   config dsw-queue-dts-profile
      edit <name>
         set iport <option>
         set oport <option>
      end
```

When this command was first added with FortiOS 6.4.6, the `iport` and `oport` options were all uppercase. However, for 6.4.8 they were converted to lower case. This change was missed in the upgrade code, so your configuration of this command may be lost after upgrading to 6.4.8.

Product integration and support

This section describes Hyperscale firewall for FortiOS 6.4.8 Build 6165 product integration and support information. The Product integration and support information described in the FortiOS 6.4.8 release notes also applies to Hyperscale firewall for FortiOS 6.4.8 Build 6165.

See the current FortiManager and FortiAnalyzer release notes for FortiManager and FortiAnalyzer compatibility.

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 6.4.8 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 6.4.8 Build 6165. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 6.4.8 release notes also apply to Hyperscale firewall for FortiOS 6.4.8 Build 6165.

Bug ID	Description
656488	Resolved an issue that could prevent FortiGate-1800F or 1801F interfaces 25 to 36, configured to operate at 10G, from connecting to some switch hardware.
684381	Resolved an issue that prevented NP7 processors from sending ICMP packets with checksum errors to the CPU. See NP7 handling of ICMP checksum errors during anomaly checking on page 7.
695803	Resolved an issue that prevented being able to change the order of DoS firewall policies from the GUI or CLI.
704851	The `config system session-ttl` command now works as a per-hyperscale firewall VDOM configuration as expected. Session timeouts set by this command only apply to the hyperscale firewall VDOM that they are added to. Global session timeouts apply to sessions in hyperscale firewall VDOMs that do not match `config system session-ttl` settings in individual hyperscale firewall VDOMs. You can also override global and per-VDOM session timeouts by setting the `tcp-timeout-pid` and `udp-timeout-pid` options in a hyperscale firewall policy.
707298 753692	Resolved an issue that caused the `snmpd` process to use relatively high amounts of CPU time when the FortiGate is not processing much traffic.
714198	Resolved an issue with how IPS re-directs NP7 offloaded sessions that can cause excess latency in transparent mode VDOMs. This issue could also block network backup traffic using port 1867.
715157	The `npu sniffer` diagnose command output now works as expected.
719779	Resolved an issue that caused interfaces that are part of a split interface to be removed from a LAG after restoring the configuration.
721294	Resolved an issue that caused incorrect traffic statistic reporting for VLAN interfaces.
722128 722547	Resolved an issue with how fragmented packets are handled by NP7 processors that caused packets to be dropped and displayed error messages on the CLI.
724061 727365	The `double-level-mcast-offload` option of the `config system npu` command now works for IPv6 multicast traffic.
724334	Resolved an issue that could prevent dynamic policy changes from correctly being implemented on the session table of the secondary FortiGate in an FGCP HA cluster.
725268 714711	IPsec traffic can now be offloaded to NP7 processors when being sent over an EMAC VLAN interface.
725502	IPsec traffic passing through virtual network interfaces is now offloaded to NP7 processors.

Bug ID	Description
725581	The `config log npu-server` command no longer generates ICMP log messages if ICMP logging is not enabled.
726326	Resolved an issue that would cause offloaded IPsec sessions to be dropped after a phase 2 re-key occurred.
727541	Resolved issues with and improved the performance of CPU or host hardware logging.
727820 729443 729616	Removed restrictions on the IP address types required or recommended when configuring hardware logging servers. You can now send log messages for any traffic type (IPv4, IPv6, NAT64, or NAT46) to any configured hardware logging server.
727907	Resolved an issue that caused both FortiGates in an FGSP cluster to create duplicate log messages for the same hardware session. The resolution prevents sessions on the secondary FortiGate from creating log messages. This means that if a failover occurs, the session will continue on the secondary FortiGate but when the sessions ends, it will not create a session end log message.
728202	The `srcaddr-negate` and `distaddr-negate` hyperscale firewall policy options now work as expected.
728299	If you disable all hyperscale firewall policies in a hyperscale firewall VDOM and then enable them in random order, SNMP queries about these policies now show correct policy statistics.
728506	You can now add a name to NAT46 and NAT64 hyperscale firewall policies.
729770 735807	Adjusted how HA failover works to make the process more efficient and faster for configurations with large numbers of VDOMs (for example, over 250 VDOMs).
730155 730527	Resolved an issue that caused the reverse deny policy to block all traffic and also helped improve performance and reduce processing errors.
730160	Resolved an issue that caused inaccurate session counts to be displayed on the GUI for individual VDOMs.
730526	Resolved an issue with how NP7 processors handle internal IPsec processing that could cause LACP/BFD/BGP flapping.
732152	Changes to `session-ttl` are now successfully applied to all sessions.
733530 728276 723824	Resolved issues with forward error correction that caused some types of traffic to be blocked.
734342	Resolved a TPE PBA leak that can prevent ARP replies from leaving FortiGate interfaces after the FortiGate has been operating for an extended period of time. As part of fixing this issue, FortiOS now checks for TPE duplication and adds a new session offload error code to the `no_ofld_reason` field of sessions that are not offloaded because of this problem. The new error code is `[NP7_FOS_ERR_DUP_TPEID] = "dup_tpe_id"`. The following diagnose command has been added to show session offload error statistics: `diag npu np7 session-offload-stats all <action>` `<action>` can be: `{0|b|brief}` show non-zero counters. `{1|v|verbose}` show all the counters.

Bug ID	Description
735269	Resolve an issue with how FortiOS handles hyperscale firewall policy changes that could cause traffic to continue to be accepted by a hyperscale firewall policy when the Action is changed to Deny All while the FortiGate is processing traffic.
735807	Resolved an issue that caused synchronization errors after creating 249 VDOMs.
737535	Resolved an issue that prevented collecting and displaying the session count for NAT64 and NAT46 sessions processed by the CPU.
738642	Resolved a kernel issue that caused the explicit proxy to drop connections and return HTTP5xx errors.
739181	Increased DoS protection capacity for CGN platforms.
739640	Improved configuration error checking when creating hardware logging servers.
740009	FortiGate-1800F and 1801F HA interfaces are now compatible with SFP connectors when the interface speed is set to 1000full.
745009	The Load Balance GUI dashboard widget is now available.
745945	The list of interfaces displayed by the `get system interface transceiver` command is now updated correctly when interfaces are split or after split interfaces are reset to their default configuration.
750149	Resolved an issue that caused NP7 processors to drop CAPWAP packets when users are authenticated using an EAP method. This was happening because the EAP packets were becoming fragmented into two packets and the second packet was smaller than the minimum allowed packet size.
750384	Resolved a number of issues with the `diagnose hardware test memory` command output.
750498	Resolved an issue with VLAN IDs and VDOM IDs that can cause fragmented packets to be dropped.
751528	Resolved an issue that caused hyperscale firewall policies to continue to allow traffic after changing the policy action to `deny` while traffic is passing through the FortiGate.
752222 753062	Resolved an issue that could cause the GUI `httpsd` process to consume excessive amounts of memory.
753390	The `config system dedicated-mgmt` command is no longer missing from FortiGates with dedicated management interfaces and NP7 processors.
753857	Resolved an issue that prevented some UDP sessions from expiring.
753869	Resolved an issue that could prevent resources from being made available after sessions expire.
754128	Resolved an issue that could cause a system to become unresponsive after creating a large number of VDOMs and firewall policies.
754362	The GUI no longer displays an error message when you change a hyperscale firewall policy Action from Accept to Deny if you have added an IP pool to the policy.
754414	Resolved an issue with how IPv6 address groups are added to NP7 processors firewall address tables.
755002 752462	Enabling the `inbandwidth` option for an interface no longer blocks all traffic from passing through that interface.
755416 755531	Resolved a multicast CPU or host logging memory leak.

Bug ID	Description
757418	Resolved an issue that could cause incorrect log rate reporting if multicast CPU or host logging is enabled.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 6.4.8 Build 6165. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 6.4.8 release notes also apply to Hyperscale firewall for FortiOS 6.4.8 Build 6165.

Bug ID	Description
724085	Traffic is blocked by EMAC-VLAN interfaces when the parent interface is in another VDOM.
728602	The GUI allows you to enable EIM in an IPv4 hyperscale firewall policy with NAT enabled and with a CGN overload IP pool. But when you save the policy and re-open it, EIM is not enabled. This configuration cannot be set up from the CLI. EIM in an IPv4 hyperscale firewall policy with NAT enabled and with a CGN overload IP pool is not supported.
728605	The CLI allows you to enable EIF for an IPv4 hyperscale firewall policy with NAT enabled and with a CGN overload IP pool. This configuration cannot be set up from the GUI. EIF in an IPv4 hyperscale firewall policy with NAT enabled and with a CGN overload IP pool is not supported.
734305	When configuring an IPv4 DoS policy from the GUI in a hyperscale firewall VDOM, the source address and destination address drop-down lists include firewall addresses that are not supported for an IPv4 DoS policy. For example, the drop down lists on the GUI may include wildcard addresses, FQDN addresses, and so on. The CLI allows you to select from the supported source and destination addresses.
757417	With per-session accounting enabled on a hyperscale firewall FGCP HA cluster, when you change the configuration of a hyperscale firewall policy that is not currently accepting traffic, the hit counter for the policy increases on the secondary FortiGate.
757420	Session synchronization to the secondary FortiGate in an FGCP hyperscale firewall HA cluster may stop working, causing the secondary FortiGate to stop responding.
758364	When operating an FGCP hyperscale firewall HA cluster, enabling or disabling Endpoint Independent Filtering (EIF) in a hyperscale firewall policy on the primary FortiGate is not synchronized to the secondary FortiGate.
759154	Enabling `srcaddr-negate` does not block traffic if the hyperscale firewall policy includes more than one source address.
759639	Per-policy accounting hit counts that are displayed on the GUI and CLI for UDP traffic are not accurate.
760010 760234	Per-policy accounting does not display hit counts on the GUI for NAT46 and NAT64 firewall policies.
760215	Established sessions may not display hit counts after per-policy accounting is enabled.
760273	Established sessions may continue to report hit counts after per-policy accounting is disabled.
760280	Enabling or disabling per-policy accounting deletes all active sessions. So enabling or disabling per-policy accounting should only be done during a quiet period.

Bug ID	Description
760560	The timestamp displayed on the GUI and CLI for the default deny policy (policy id = 0) in a hyperscale firewall VDOM is incorrect.