Hyperscale Firewall - Release Notes

Version 6.4.6 Build 5868

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

FORTINET®

January 11, 2023
Hyperscale Firewall 6.4.6 Build 5868 Release Notes
01-646-724638-20230111

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 6.4.6 incompatibilities and limitations on page 15.
February 14, 2022	New section: Check the NP queue priority configuration after a firmware upgrade on page 13. Also, a note has been added about this issue to, Upgrade information on page 18.
December 17, 2021	Corrected the description of the `vlan-lookup-cache` option of the `config system npu` command in New config system npu options on page 7.
December 2, 2021	Add two new FGCP HA-related limitations to Hyperscale firewall 6.4.6 incompatibilities and limitations on page 15.
October 18, 2021	Removed the incorrect statement "NP7 fragment reassembly is not supported" from Hyperscale firewall 6.4.6 incompatibilities and limitations on page 15. See Reassembling fragmented packets for information about supporting NP7 fragment reassembly. Corrected the section Setting the hyperscale firewall VDOM default policy action on page 7.
September 30, 2021	Added the FortiGate-3500F and 3501F to Supported FortiGate models on page 5.
August 23, 2021	Added known issue 740225 to Known issues on page 23.
August 17, 2021	Some corrections to Known issues on page 23. Including removing 721246 and correcting 727391.
July 14, 2021	Added all Known issues on page 23.
July 13, 2021	Added more Known issues on page 23.
July 12, 2021	Added all known Resolved issues on page 20. Added more Known issues on page 23. Updated Product integration and support on page 19. Misc fixes and additions to What's new on page 6.
July 9, 2021	Initial version.

Hyperscale firewall for FortiOS 6.4.6 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 6.4.6 Build 5868.

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 6.4.6 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 6.4.6 Build 5868.

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

Supported FortiGate models

Hyperscale firewall for FortiOS 6.4.6 Build 5868 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-3500F (build 6135)
- FortiGate-3501F (build 6135)
- FortiGate-4200F
- FortiGate-4201F
- FortiGate-4400F
- FortiGate-4401F

What’s new

The following new features have been added to Hyperscale firewall for FortiOS 6.4.6 Build 5868. 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 6.4.6 release notes also apply to Hyperscale firewall for FortiOS 6.4.6 Build 5868.

Multicast logging

You can use multicast logging to simultaneously send session setup log messages for CPU or software sessions to multiple remote syslog or NetFlow servers. Multicast logging is not supported for NP7 sessions.

Enable multicast logging by creating a log server group that contains two or more remote log servers and then set `log-tx-mode` to `multicast`:

```
config log npu-server
   set log-processor {hardware | host}
      config server-group
         edit "log_ipv4_server1"
            set log-format {netflow | syslog}
            set log-tx-mode multicast
         end
```

The following example shows how to set up two remote syslog servers and then add them to a log server group with multicast logging enabled.

```
config log npu-server
   set log-processor {hardware | host}
      config server-info
         edit 1
            set vdom "root"
            set ipv4-server <server-ip>
            set source-port 8055
            set dest-port 2055
            set template-tx-timeout 60
         next
         edit 2
            set vdom "root"
            set ipv4-server <server-ip>
            set source-port 8055
            set dest-port 2055
            set template-tx-timeout 60
         end
      end
   config server-group
      edit "Example-Multicast"
         set log-format syslog
         set log-tx-mode multicast
         set server-number 2
         set server-start-id 1
```

```
    end
```

Setting the hyperscale firewall VDOM default policy action

You can use the following system settings option for each hyperscale firewall VDOM to set the hyperscale firewall default policy action for that VDOM. The hyperscale policy default action determines what NP7 processors do with TCP and UDP packets that are not accepted by any hyperscale firewall policies.

```
config system setting
   set hyperscale-default-policy-action {drop-on-hardware | forward-to-host}
end
```

`drop-on-hardware` the default setting, NP7 processors drop TCP and UDP packets that don't match a hyperscale firewall policy. In most cases you would not want to change this default setting since it means the CPU does not have to process TCP and UDP packets that don't match hyperscale firewall policies. In most cases, this option should reduce the number of packets sent to the CPU. With this option enabled, all other packet types (for example, ICMP packets) that don't match a hyperscale firewall policy are sent to the CPU. Packets accepted by session helpers are also sent to the CPU.

`forward-to-host` NP7 processors forward packets that don't match a hyperscale firewall policy to the CPU. If the packet is forwarded to the CPU, the packet will be matched with the policy list and eventually be subject to the implicit deny policy and dropped by the CPU. This setting can affect performance because the CPU would be handling these packets.

New config system npu options

The following new options have been added to the `config system npu` command for NP7 platforms for FortiOS 6.4.6:

```
config system npu
   set tcp-rst-timeout <timeout>
   set napi-break-interval <interval>
   set vlan-lookup-cache {disable | enable}
   set htab-msg-queue {data | idle | dedicated}
   set htab-dedi-queue-nr <number-of-queues>
   set double-level-mcast-offload {disable | enable}
end
```

`tcp-rst-timeout` the NP7 TCP reset (RST) timeout in seconds. The range is 0-16777215. The default timeout is 5 seconds. This timeout is optimal in most cases, especially when hyperscale firewall is enabled. A timeout of 0 means no time out.

`napi-break-interval` set the new API (NAPI) break interval. The range is 0 to 65535. The default interval is 0.

`vlan-lookup-cache` enable or disable VLAN lookup (SPV/TPV) caching. Enable this option to optimize performance of NP7-offloaded traffic passing through VLAN interfaces. This option is enabled by default. Enabling or disabling `vlan-lookup-cache` requires a system restart. You should only change this setting during a maintenance window or quiet period.

`htab-msg-queue` hash table message queue mode. You can use this option to alleviate performance bottlenecks that may occur when hash table messages use up all of the available hyperscale NP7 data queues.

You can use the following commands to get the hash table message count and rate.

```
diagnose npu np7 msg htab-stats {all| chip-id}
diagnose npu np7 msg htab-rate {all| chip-id}
```

You can use the following command to show MSWM information:

```
diagnose npu np7 mswm
```

You can use the following command to show Session Search Engine (SSE) drop counters:

```
diagnose npu np7 dce-sse-drop 0 v
```

You can use the following command to show command counters:

```
diagnose npu np7 cmd
```

The following `htab-msg-queue` options are available:

- `data` (the default) use all available data queues.
- `idle` if you notice the data queues are all in use, you can select this option to use idle queues for hash table messages.
- `dedicated` use between 1 to 8 of the highest number data queues. Use the option `htab-dedi-queue-nr` to set the number of data queues to use.

`htab-dedi-queue-nr` if you are using dedicated queues for hash table messages for hyperscale firewall sessions, you can set the number of queues to use. The range is 1 to 8 queues. The default is 4 queues.

`double-level-mcast-offload` enable to support NP7 offloading for more than 256 destinations for multicast replication. By default this option is disabled and NP7 processors support up to 256 destinations for multicast replication. You can enable this option to effectively double the number.

Message-related diagnose commands:

```
diagnose npu np7 msg
summary          Show summary of message counters. [Take 0-1 arg(s)]
msg-by-mod       Show/clear message counters by source module. [Take 0-2 arg(s)]
msg-by-code      Show/clear message counters by message code. [Take 0-2 arg(s)]
msg-by-que       Show/clear message counters by RX queue. [Take 0-2 arg(s)]
msg-by-cpu       Show/clear message counters by CPU. [Take 0-2 arg(s)]
htab-stats       Show/clear hash table message counters. [Take 0-2 arg(s)]
htab-rate        Show/clear hash table message rate. [Take 0-2 arg(s)]
ipsec-stats      Show/clear IPSec message counters. [Take 0-2 arg(s)]
ipsec-rate       Show/clear IPSec message rate. [Take 0-2 arg(s)]
ipt-stats        Show/clear IP tunnel message counters. [Take 0-2 arg(s)]
ipt-rate         Show/clear IP tunnel message rate. [Take 0-2 arg(s)]
mse-stats        Show/clear MSE message counters. [Take 0-2 arg(s)]
mse-rate         Show/clear MSE message rate. [Take 0-2 arg(s)]
spath-stats      Show/clear hyperscale message counters. [Take 0-2 arg(s)]
spath-rate       Show/clear hyperscale message rate. [Take 0-2 arg(s)]
tpe-tce-stats    Show/clear TPC/TCE message counters. [Take 0-2 arg(s)]
tpe-tce-rate     Show/clear TPE/TCE message rate. [Take 0-2 arg(s)]
```

MSWM diag commands.

```
diagnose npu np7 mswm
mswm-all          Show/clear all MSWM counters. [Take 0-2 arg(s)]
module-to-mswm    Show/clear module-to-MSWM counters. [Take 0-2 arg(s)]
mswm-to-module    Show/clear MSWM-to-module counters. [Take 0-2 arg(s)]
mswh-all          Show/clear all MSWH counters. [Take 0-2 arg(s)]
```

```
module-to-mswh    Show/clear module-to-MSWH counters. [Take 0-2 arg(s)]
mswh-to-hrx       Show/clear MSWH-to-HRX counter. [Take 0-2 arg(s)]
```

Diagnose command to show SSE drop counters:

```
diagnose npu np7 dce-sse-drop 0 v
```

Diagnose command to show command counters:

```
diagnose npu np7 cmd
all             Show/clear all command counters. [Take 0-2 arg(s)]
sse             Show/clear SSE command counters. [Take 0-2 arg(s)]
mse             Show/clear MSE command counters. [Take 0-2 arg(s)]
dse             Show/clear DSE command counters. [Take 0-2 arg(s)]
lpm-rlt         Show/clear LPM/RLT command counters. [Take 0-2 arg(s)]
rate            Show/clear command rate. [Take 0-2 arg(s)]
measure-rate    Enable/disable command rate measurement. [Take 0-1 arg(s)]
```

HPE changes

The NP7 host protection engine (HPE) has been redesigned to apply DDoS protection according to each NPU host queue. This new design should result in more accurate and reliable protection for different network topologies

Use the following command to configure the NP7 host protection engine (HPE) to apply DDoS protection by limiting the number of packets per second received for various packet types per host queue by each NP7 processor. This rate limiting is applied very efficiently because it is done in hardware by the NP7 processor.

```
config system npu
   config hpe
      set all-protocol <packets-per-second>
      set tcpsyn-max <packets-per-second>
      set tcpsyn-ack-max <packets-per-second>
      set tcpfin-rst-max <packets-per-second>
      set tcp-max <packets-per-second>
      set udp-max <packets-per-second>
      set icmp-max <packets-per-second>
      set sctp-max <packets-per-second>
      set esp-max <packets-per-second>
      set ip-frag-max <packets-per-second>
      set ip-others-max <packets-per-second>
      set arp-max <packets-per-second>
      set l2-others-max <packets-per-second>
      set high-priority <packets-per-second>
      set enable-shaper {disable | enable}
   end
```

Command	Description	Default
enable-shaper {disable | enable}	Enable or disable HPE DDoS protection.	disable
all-protocol	Maximum packet rate of each host queue for all traffic except high priority traffic. The range is 0 to 40000000 pps. Set to 0 to disable.	400000
tcpsyn-max	Limit the maximum number of TCP SYN packets received per second.	40000

Command	Description	Default
	The range is 1000 to 40000000 pps.	
`tcpsyn-ack-max`	Prevent SYN_ACK reflection attacks by limiting the number of TCP SYN_ACK packets received per second. The range is 1000 to 40000000 pps. TCP SYN_ACK reflection attacks consist of an attacker sends large amounts of SYN_ACK packets without first sending SYN packets. These attacks can cause high CPU usage because the 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.	40000
`tcpfin-rst-max`	Limit the maximum number of TCP FIN and RST packets received per second. The range is 1000 to 40000000 pps.	40000
`tcp-max`	Limit the maximum number of TCP packets received per second that are not filtered by `tcpsyn-max`, `tcpsyn-ack-max`, or `tcpfin-rst-max`. The range is 1000 to 40000000 pps.	40000
`udp-max`	Limit the maximum number of UDP packets received per second. The range is 1000 to 40000000 pps.	40000
`icmp-max`	Limit the maximum number of ICMP packets received. The range is 1000 to 40000000 pps.	20000
`sctp-max`	Limit the maximum number of SCTP packets received. The range is 1000 to 40000000 pps.	20000
`esp-max`	Limit the maximum number of ESP packets received. The range is 1000 to 40000000 pps.	20000
`ip-frag-max`	Limit the maximum number of fragmented IP packets received. The range is 1000 to 40000000 pps.	20000
`ip-others-max`	Limit the maximum number of other types of IP packets received. Other packet types cannot be set with other HPE options. The range is 1000 to 40000000 pps.	20000
`arp-max`	Limit the maximum number of ARP packets received. The range is 1000 to 40000000 pps.	20000
`l2-others-max`	Limit the maximum number of other layer-2 packets that are not ARP packets. The range is 1000 to 40000000 pps. This option limits the following types of packets: HA heartbeat and session sync, LACP/802.3ad, FortiSwitch heartbeat, and wireless-controller CAPWAP.	20000
`high-priority`	Set the maximum overflow limit for high priority traffic. The range is 1000 to 40000000 pps. This overflow is applied to the following types of traffic that are treated as high-priority by the NP7 processor: • HA heartbeat • LACP/802.3ad	40000

Command	Description	Default
	• OSPF • BGP • IKE • SLBC • BFD This option adds an overflow for high priority traffic, causing the HPE to allow more of these high priority packets to be accepted by the NP7 processor. The overflow is added to the maximum number of packets allowed by HPE based on the other HPE settings. For example, the NP7 processor treats IKE traffic as high priority; so the HPE limits IKE traffic to `udp-max` + `pri-type-max` pps, which works out to 125000 + 40000 = 165000 pps. In some cases, you may not want the overflow to apply to BGP, SLBC or BFD traffic. See HPE changes on page 9 for details.	

HPE diagnose command

Use the following command to display HPE configuration and status information The command displays information for a single NP7 processor, by default NP7_0. You can optionally include the NP ID to display information for one of the other NP7 processors. The following command displays information for NP7_2..

```
diagnose npu np7 hpe 2

[NP7_2]
Queue  Type          NPU-min   NPU-max   CFG-min(pps) CFG-max(pps) Pkt-credit
0      high-priority39731     39731     40000        40000        0
0      TCP-syn       39731     39731     40000        40000        0
0      TCP-synack    39731     39731     40000        40000        0
0      TCP-finrst    39731     39731     40000        40000        0
0      TCP           39731     39731     40000        40000        0
0      UDP           39731     39731     40000        40000        0
0      ICMP          19865     19865     20000        20000        0
0      SCTP          19865     19865     20000        20000        0
0      ESP           19865     19865     20000        20000        0
0      IP-Frag       19865     19865     20000        20000        0
0      IP_others     19865     19865     20000        20000        0
0      ARP           19865     19865     20000        20000        0
0      l2_others     19865     19865     20000        20000        0
0      all-protocol 39731     39731     40000        40000        0
---------------------------------------------------------------------------
HPE HW pkt_credit:11080 , tsref_inv:50000, tsref_gap:32, hpe_refskip:0 , hif->nr_ring:40

Note:
 NPU-min and NPU-max: The register reading of max and min value for each queue in NPU.
 CFG-min(pps): the setting value of hpe configuration in CLI command and
               it is packet per second rate limit for each host rx queue of NPU.
 CFG-max(pps): The value is CFG-min of hpe configuration in CLI command.
```

Monitoring HPE activity

You can use the following command to generate event log messages when the HPE drops packets:

```
config monitoring npu-hpe
   set status {disable | enable}
   set interval <interval>
   set multipliers <12*multipliers>
end
```

`status` enable or disable HPE status monitoring.

`interval` HPE status check interval in seconds. The range is 1 to 60 seconds. The default interval is 1 second.

`multipliers` set 12 multipliers to control how often an even log is generated for each HPE option in the following order:

1. `tcpsyn-max` default 4
2. `tcpsyn-ack-max` default 4
3. `tcpfin-rst-max` default 4
4. `tcp-max` default 4
5. `udp-max` default 8
6. `icmp-max` default 8
7. `sctp-max` default 8
8. `esp-max` default 8
9. `ip-frag-max` default 8
10. `ip-others-max` default 8
11. `arp-max` default 8
12. `l2-others-max` default 8

An event log is generated after every (`interval` * `multiplier`) seconds for each HPE option when drops occur for that HPE type. Increase the interval or individual multipliers to generate fewer event log messages.

An attack log is generated after every (4 * `multiplier`) continuous event logs.

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 6.4.6 Build 5868. The Special notices described in the FortiOS 6.4.6 release notes also apply to Hyperscale firewall for FortiOS 6.4.6 Build 5868.

Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 6.4.6, 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
```

Hardware logging server IP address restrictions

When configuring hardware logging, the recommended or required IP addresses of the hardware logging servers that you can use with hyperscale firewall policies are the following:

- You should only use logging servers that have IPv4 addresses with IPv4 hyperscale firewall policies. Logging servers with IPv6 IP addresses can be used but are not recommended.
- You should only use logging servers that have IPv6 addresses with IPv6 hyperscale firewall policies. Logging servers with IPv4 IP addresses can be used but are not recommended.
- You can only use logging servers that have IPv6 addresses with NAT64 hyperscale firewall policies.
- You can only use logging servers that have IPv4 addresses with NAT46 hyperscale firewall policies.

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 6.4.6 incompatibilities and limitations

Hyperscale firewall for FortiOS 6.4.6 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 6.4.6 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 or 6.2.7 firmware and is licensed for hyperscale firewall features, you can follow a normal firmware upgrade process to upgrade to FortiOS 6.4.6.

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 6.4.6. To configure hyperscale firewall features, activate your hyperscale firewall license and set up the 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 13.

Product integration and support

This section describes Hyperscale firewall for FortiOS 6.4.6 Build 5868 product integration and support information. The Product integration and support information described in the FortiOS 6.4.6 release notes also applies to Hyperscale firewall for FortiOS 6.4.6 Build 5868.

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

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 6.4.6 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 6.4.6 Build 5868. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 6.4.6 release notes also apply to Hyperscale firewall for FortiOS 6.4.6 Build 5868.

Bug ID	Description
662514	Improved handling of NAT46 traffic to prevent problems caused by the frame size increase resulting from converting an IPv4 packet to an IPv6 packet.
664828	Resolved an NP7 driver issue that prevented L2TP VPN from working.
689384	Resolved an issue that prevented offloading VXLAN over IPsec traffic.
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.
714800 725190 727179	Resolved an issue that caused NPD process timeouts on the secondary FortiGate in an FGCP cluster after editing a hyperscale firewall policy and changing the CGN IP pool used in the policy.
716379	The GUI now accurately shows that the FortiGate-4200F, 4201F, 4400F, and 4401F ha1, ha2, aux1, and aux2 interfaces are in the same port or interface group.
717304	Resolved an issue that caused the time displayed by the real time clock to be inaccurate. Fortinet recommends enabling NTP to make sure FortiGate system time is accurate.
720595	Hyperscale firewall hardware logging now supports more than ten hardware logging servers.
721246	Resolved an issue that prevented adding custom service groups to hyperscale firewall policies.
721442	Resolved an issue that prevented the `diagnose npu np7 gtp-stats-all` and `diagnose npu np7 gtp-stats <np#>` commands from displaying output on the primary FortiGate in an FGCP cluster when GTP enhanced mode is enabled.
722375	Resolved an NP7 issue with GTP enhanced mode that could block GTP-U traffic.
723947	The `diagnose sys npu-session purge` command now works as expected to clear all NPU sessions.
724638 721328	Fixes to DSE hit logic.
725975 722687	Hyperscale firewall policy usage statistics now display on the GUI when editing a policy.
726262	The GUI will no longer display an error message when you edit the first port number in a port number range in a CGN resource allocation IP pool.
718356	BGP prefixes are now successfully cleared from the NP7 routing table after they have been removed from the kernel because the peer they point to has gone down.
711135	Resolved synchronization issues that caused various HA-related performance reductions or

Bug ID	Description
717564 716766 722922 726265	unexpected behavior.
718257	Resolved an issue that prevented NP7 processors from synchronizing the OSPF FIB when the route update rate is high.
716304	Improved power monitoring to reduce reporting false positives. For example, the FortiGate will now check multiple times if an error is received, and only report an error if the error condition persists.
716094	Resolved an issue that could disrupt traffic when enabling per-IP traffic shaping and `max-concurrent-session` for a firewall policy with NP7 offloading enabled.
709046	Resolved an issue that could cause inaccurate statistics reporting when the system is processing a large number of sessions.
715532	Resolved an index limit issue that prevented being 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).
716424	Resolved an issue that caused the NPD process to crash 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.
718886	When the SIP session helper is enabled, SIP traffic is offloaded to NP7 processors.
717011	Resolved an issue that could cause SIP ALG traffic to produce PBA leaks and deadlocks.
720592	Resolved an issue that caused hardware sessions to expire on the secondary FortiGate in an FGCP HA cluster.
714915	Changing the configuration of a hardware log server group assigned to a hyperscale firewall policy that is processing traffic no longer causes sessions accepted by the firewall policy to be dropped.
720616	Resolved an issue that caused the system to create unexpected UDP sessions after changing the hardware host logging configuration.
721231	Resolved an issue that caused IPsec VPN sessions between VDOMs to timeout while they are processing traffic.
720203	Resolved an issue that caused session helper sessions to be offloaded to NP7 processors after changing the IP pool in a hyperscale firewall policy.
723551	Resolved an issue that could prevent TFTP ALG sessions from being offloaded to NP7 processors.
718713	Configuring an interface to drop fragmented packets (`drop-fragment` set to `enable`) now works as expected.
718046	Resolved an issue that blocked traffic going through a virtual network interface.

Bug ID	Description
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: `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 "`
719794	Resolved an issue that could prevent the IP Pool option from appearing in a hyperscale firewall policy.
725978	Sync session count information has been added to the output of the `get system ha status` command.
725343	Messages similar to `NPD vd=x get tmo id=xxxx fail!` no longer appear after restoring the configuration.
708028	Resolved an issue that caused the generation of `NPD firewall policy offload failed` event log messages.
726531	The log rate is no longer displayed as a negative value after changing hardware logging to host logging mode.
725581	Resolved an issue that sometimes causes ICMP logs to be generated for traffic accepted by a hyperscale firewall policy with logging disabled.
725094	SNMP queries of IPv6 hyperscale firewall policies work as expected.
726542	Resolved an issue that was keeping software sessions in the session table after traffic has stopped.
725584	Resolved an issue that caused excessive memory use when adding and deleting BGP routes.
728822	Resolved a memory leak related to hardware logging.
729142	Resolved a PBA memory leak.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 6.4.6 Build 5868. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 6.4.6 release notes also apply to Hyperscale firewall for FortiOS 6.4.6 Build 5868.

Bug ID	Description
704851	The `config system session-ttl` 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.
720247	MAC filter drops sometimes appear on SIP traffic.
727145	Some CPUs or NP7 processors may get stuck from fifo deadlocks and hw/sw session conflicts.

727391	For optimal performance, the following option should be set to `disable` if your configuration includes 256 or more VLANs:
	`config system npu`
	`   set vlan-lookup-cache {disable | enable}`
	`end`
	Enabling or disabling `vlan-lookup-cache` requires a system restart. So you should only change this setting during a maintenance window.

728299	If you disable all hyperscale firewall policies in a VDOM and then enable them in random order, SNMP queries about these policies will show incorrect policy IDs.
729627	After an HA failover, sessions in the new primary FortiGate are incorrectly labeled as native sessions when they are sync-over sessions.
729645	In some cases, left over UDP IPv4 sessions are not cleared from the sessions list.
731041	Hyperscale firewall sessions using fixed allocation IP pools may be dropped during an FGCP HA failover.
725502	Traffic passing through virtual network interfaces is not offloaded to NP7 processors.
730238	Configurations with large number of VDOMs may cause NPD UNKNOW ERRNO errors.
730441	Processing large amounts of IPv6 multicast traffic over extended time periods may cause the FortiGate to restart.
727277	Error messages may appear on the CLI console after adding or deleting transparent mode VDOMs.
729443	NAT64 hyperscale firewall policies will be lost after upgrading from FortiOS 6.2.7 build 7105 to 6.4.6 Build 5868, if the NAT64 policies are configured to send hardware log messages to a log server with an IPv4 IP address. You can work around this issue by replacing the IPv4 log server with an IPv6 log server before upgrading.
729616	The GUI and CLI allow you to incorrectly configure IPv4 hyperscale firewall policies that include a hardware logging server with an IPv6 IP address. For more information, see Hardware logging server IP address restrictions on page 15.

Bug ID	Description
728583	WCCP firewall policies will block traffic if an IPS sensor has been added to the policy and `np-accleration` is also enabled. The traffic is blocked because of an issue with NTurbo. You can work around this issue by disabling `np-acceleration`.
727283	The GUI menu of an FGCP HA cluster can show duplicate **Dashboard > Status** entries.
728629	Hyperscale sessions matched with policy routes may not be successfully offloaded if the source address of the policy route is added to the IP/Netmask field. Sessions accepted by policy routes where the source address is one or more firewall address added to the Addresses field should work as expected.
729062	Including IPv4 and IPv6 firewall addresses in the same hyperscale firewall policy will not work as intended. Instead, you should create separate IPv4 and IPv6 hyperscale firewall policies.
728439	ECMP load balancing may not work as expected in the reply direction. Instead of traffic being load balanced between multiple destinations, all traffic uses the same destination.
728307	When viewing information about a hardware log server from the GUI, the Ref. column does not contain a list of the policies that the hardware log server has been added to.
728202	The `srcaddr-negate` and `distaddr-negate` hyperscale firewall policy options have no effect.
728506	NAT46 and NAT64 hyperscale firewall policies do not include a Name field.
727889	NAT46 and NAT64 UDP packets can intermittently be dropped.
724964	Configuring load balancing by creating multiple policy routes with the same priority and destination does not work as expected. Traffic is not load balanced, but all traffic uses one of the policy routes.
728011	The secondary FortiGate in an FGCP HA cluster displays debug messages on the CLI console when the FortiGate is added to a cluster.
728136	For an FGCP HA cluster, the output of the `diagnose sys npu-session stat` command always indicates that the hit count is 0.
727052	In some cases, user TCP sessions expire counters are not updated in a hyperscale firewall VDOM when the sessions receive new traffic. As a result, the session expires and has to be restarted.
727465	Transparent mode hyperscale firewall VDOMs may behave in unexpected ways leading to some or all traffic being dropped.
727219	IPv6 UDP traffic may be forwarded by the secondary FortiGate in an FGCP HA A-P cluster.
727288	In some cases, the `diagnose sys npu-session list` command takes longer than normal to display results and may display incorrect information.
718693	In some configurations, fragmented packets are unexpectedly sent to the CPU instead of NP7 processors.
718442	SNMP queries for NAT64 session counts may not return any data.
706696	SNMP UDP traffic passing through a FortiGate may be dropped when NP7 hardware acceleration is enabled.
724336	Disabling `service-negate` when editing a hyperscale firewall policy can cause error messages to appear on the CLI console.

Bug ID	Description
724334	In some cases, some sessions are not removed from the secondary FortiGate in an FGCP HA cluster when they expire on the primary FortiGate.
718717	Packets may not be fragmented when they leave an inter-VDOM link interface and the packets are larger than the MTU of the interface.
724085	Traffic fails over an EMAC VLAN interface when the source interface is in another VDOM.
730898	TCP traffic may be incorrectly blocked by a specific policy that doesn't match the traffic, but has been added above a general policy that would accept the traffic.
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 workaround 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.