Hyperscale Firewall - Release Notes

Version 6.2.9 Build 7197

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 6.2.9 Build 7197 Release Notes
01-629-737193-20230111

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 6.2.9 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	Added two new FGCP HA-related limitations to Hyperscale firewall 6.2.9 incompatibilities and limitations on page 15.
October 18, 2021	Removed the incorrect statement "NP7 fragment reassembly is not supported" from Hyperscale firewall 6.2.9 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 6.
August 23, 2021	Added known issue 740225 to Known issues on page 25.
August 17, 2021	Fixed some links.
August 16, 2021	Initial version.

Hyperscale firewall for FortiOS 6.2.9 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 6.2.9 Build 7197.

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 6.2.9 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 6.2.9 Build 7197.

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

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

Supported FortiGate models

Hyperscale firewall for FortiOS 6.2.9 Build 7197 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 6.2.9 Build 7197.

Hyperscale firewall VDOM asymmetric routing with ECMP support

Hyperscale firewall VDOMs for FortiOS 6.2.9 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.

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 6.2.9:

```
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 disabled 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. The range is 1000 to 40000000 pps.	40000
`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

Command	Description	Default
`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 • 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 8 for details.	40000

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 6.2.9 Build 7197. The Special notices described in the FortiOS 6.2.9 release notes also apply to Hyperscale firewall for FortiOS 6.2.9 Build 7197.

Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 6.2.9, 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.

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.

Hyperscale firewall 6.2.9 incompatibilities and limitations

Hyperscale firewall for FortiOS 6.2.9 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 6.2.9 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 13.

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 6.2.9.

If you are currently operating a FortiGate-4200F, 4201F, 4400F, or 4401F running FortiOS 6.2.5 or older and a hyperscale firewall license, you can upgrade in one step to FortiOS 6.2.9 because upgrading to FortiOS 6.2.9 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 6.2.9.

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 6.2.9. To configure hyperscale firewall features, activate your hyperscale firewall license and set up the hyperscale firewall configuration.

The FortiOS 6.2.9 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 6.2.9 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 FortiOS 6.2.5 and older

Recommended procedure for upgrading an HA cluster from FortiOS 6.2.5 and older to FortiOS 6.2.9:

1. Disconnect the backup FortiGate from the cluster.
2. Upgrade the backup FortiGate's firmware to FortiOS 6.2.9 and set the configuration to factory defaults.
3. Create the new FortiOS 6.2.9 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 FortiOS 6.2.5 and older

To upgrade a standalone FortiGate from FortiOS 6.2.5 and older to FortiOS 6.2.9, 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 6.2.9 Build 7197 product integration and support information. The Product integration and support information described in the FortiOS 6.2.9 release notes also applies to Hyperscale firewall for FortiOS 6.2.9 Build 7197.

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

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 6.2.9 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 6.2.9 Build 7197. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 6.2.9 release notes also apply to Hyperscale firewall for FortiOS 6.2.9 Build 7197.

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.
695803	Resolved an issue that prevented being able to change the order of DoS firewall policies from the GUI or CLI.
707298	Resolved an issue that would periodically cause the `snmpd` process to use excessive amounts of CPU time.
709046	Resolved an issue that could cause inaccurate statistics reporting when the FortiGate is processing a large number of sessions.
711135 722922	Resolved synchronization issues that caused various HA-related performance reductions or unexpected behavior.
712023 713415	Resolved an issue that prevented IPS from scanning traffic in a CAPWAP tunnel when DTLS and nTurbo is enabled.
712221	Resolved an issue that caused SSH management sessions to disconnect after entering the command `diagnose traffictest set_pair aggregateInt`.
713432 727173	Adjusted the CPU/Memory Performance Test threshold so that the test can find meaningful results, which are then displayed by the `diagnose hardware test info` command.
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.
714800	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.
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.
715090	Resolved an issue that prevented the FortiGate-2600F and 2601F from displaying the default fortilink interface on the GUI or CLI.
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.
716169	SPF interfaces with speed set to 1000full no longer remain down after the system restarts.
716766 717564	Resolved synchronization issues that caused various HA-related performance reductions or unexpected behavior.

Bug ID	Description
718713	Configuring an interface to drop fragmented packets (`drop-fragment` set to `enable`) now works as expected.
718886	When the SIP session helper is enabled, SIP traffic is offloaded to NP7 processors.
719794	Resolved an issue that could prevent the IP Pool option from appearing in a hyperscale firewall policy.
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.
720592	Resolved an issue that caused hardware sessions to expire on the secondary FortiGate in an FGCP HA cluster.
720595	Hyperscale firewall hardware logging now supports more than ten hardware logging servers.
721231	Resolved an issue that caused IPsec VPN sessions between VDOMs to timeout while they are processing traffic.
721246 721282	Resolved an issue that prevented adding custom service groups to hyperscale firewall policies.
721328	Fixes to DSE hit logic.
721349	Resolved an issue that could cause a WiFi client to disconnect after connecting to a WiFi interface with a tunnel SSID.
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.
722128 722547	Improved fragmented packet handling to prevent dropped packets when fragment SKB size is relatively small.
722375	Resolved an NP7 issue with GTP enhanced mode that could block GTP-U traffic.
723551	Resolved an issue that could prevent TFTP ALG sessions from being offloaded to NP7 processors.
725268 714711	IPsec traffic can now be offloaded when being sent over an EMAC VLAN interface.
725343	Messages similar to `NPD vd=x get tmo id=xxxx fail!` no longer appear after restoring the configuration.
725581	The `config log npu-server` command no longer generates ICMP log messages if ICMP logging is not enabled.
725978	Sync session count information has been added to the output of the `get system ha status` command.
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.
726265	Resolved synchronization issues that caused various HA-related performance reductions or unexpected behavior.

Bug ID	Description
726531	The log rate is no longer displayed as a negative value after changing hardware logging to host logging mode.
726542	Resolved an issue that was keeping software sessions in the session table after traffic has stopped.

727391	Resolved an issue that caused PBA leaks with the FortiGate is configured with a large number of VLANs (for example, 1000 VLANs).
	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. This option is disabled by default.

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.
728453	Resolved an issue that could cause the `npd` process to crash when editing CGN IP pools. This issue can also cause packets to be stuck. You can use the `diagnose npu np7 setreg` command to enable a watch dog and adjust the threshold for releasing stuck packets.
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.
734342	Resolved an NP7-related issue caused by some traffic shaping configurations that could cause FortiGate interfaces to become unresponsive because ARP replies will no longer be sent by FortiGate interfaces. Added a new command `diagnose npu np7 session-offload-stats all`that will display statistics that include NP7 session offloading errors.
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 software.
737112	Resolved and issue that prevented deleting multiple VDOMs when CPU or host hardware logging is enabled.

Common vulnerabilities and exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
677844	Hyperscale firewall for FortiOS 6.2.9 SSL VPN portal is no longer vulnerable to an XSS.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 6.2.9 Build 7197. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 6.2.9 release notes also apply to Hyperscale firewall for FortiOS 6.2.9 Build 7197.

Bug ID	Description
669645	VXLAN interfaces cannot be added to a hardware switch interface.
707356	SNMP results only show the IPv4 session count and the number of sessions is a total of the IPv4, IPv6, NAT64, and NAT46 sessions.
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.
724085	Traffic fails over an EMAC VLAN interface when the source interface is in another VDOM.
731168	In some cases the GUI will take a long time to load the page or display an error message when attempting to edit an interface or create a new interface.
732380	It takes longer than expected for hardware sessions to use a policy route after the policy route is enabled.
734305	The GUI may allow you to select invalid firewall addresses when adding source or destination addresses to an IPv4 or IPv6 DoS Policy.
734486	In a hyperscale VDOM, the GUI displays the error message "You have no firewall policies configured. Click here to create a new firewall policy." because the GUI is looking for standard firewall policies which cannot be created in a hyperscale VDOM.
736635	After setting `log-processor` to `host` when configuring hardware logging, the output of the `diagnose sys npu-session stat` and `diagnose sys npu-session list` commands show hardware session counts of 0 when the FortiGate is processing hardware sessions.
737059	After changing an IP pool, it may take more time than expected for all sessions using the IP pool when it was changed to be re-established.
738925	The GUI can become unresponsive if CPU usage becomes high, for example over 97%. CLI access using SSH still works as expected and FortiGate interfaces will respond to ping requests. The GUI can become unresponsive with high CPU usage even if you have enabled the dedicated management CPU feature.
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.