Hyperscale Firewall - Release Notes

Version 6.4.10 Build 2000

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 6.4.10 Build 2000 Release Notes
01-6410-836251-20230111

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 6.4.11 incompatibilities and limitations on page 10.
August 25, 2022	Initial version.

Hyperscale firewall for FortiOS 6.4.11 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 6.4.10 Build 2000.

In addition, special notices, changes in default behavior,new features and enhancements, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 6.4.10 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 6.4.10 Build 2000.

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 6.4.10 Build 2000 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 6.4.10 Build 2000. The changes in default behavior, and new features or enhancements described in the FortiOS 6.4.10 release notes also apply to Hyperscale firewall for FortiOS 6.4.10 Build 2000.

Hyperscale firewall policy engine enhancements

Hyperscale Firewall 6.4.11 includes a re-worked hyperscale firewall policy engine. This section describes some of the features of the new policy engine and some limitations and implementation details of how it functions.

The NP7 hyperscale firewall policy engine is also called the Policy Lookup Engine (PLE). The PLE handles processing of all hyperscale firewall policies in all hyperscale firewall VDOMs. When the hyperscale firewall policy configuration changes, the PLE compiler creates a new policy database (also called a policy set) that is used by NP7 processors to apply hyperscale firewall and carrier grade NAT (CGN) features to offloaded traffic.

Hyperscale firewall policy maximum values

The following maximum values are global limits for all hyperscale VDOMs and are not per individual VDOMs. These maximum values have been tested for FortiOS 6.4.11 and may be changed in the future as the result of ongoing and future optimizations.

- The maximum number of hyperscale firewall policies allowed in the policy database: 20,000.
- The maximum number of IP-ranges specified by firewall addresses that can be added to a single hyperscale firewall policy: 2000.
- The maximum number of IP-ranges that can be added to the firewall policy database: 32,000.
- The maximum number of port-ranges specified by firewall addresses that can be added to a single hyperscale firewall policy: 1,000.
- The maximum number of port-ranges that can be added to the firewall policy database: 4,000.

The maximum number of hyperscale firewall policies allowed in a VDOM is controlled by the maximum value for the number of firewall policies allowed per VDOM for your FortiGate.

Additional considerations

The factors that affect whether a hyperscale policy database can be supported or not includes but are not limited to:

- The total number of hyperscale firewall policies.
- The total number of IP-ranges and port-ranges as defined by firewall addresses added to hyperscale firewall

policies in the firewall policy database
- The relationship between policies, such as how IP-ranges are distributed among hyperscale firewall policies.

It is possible to create a hyperscale policy database that is within the maximum values but cannot be supported. If this happens, FortiOS will create an error message when the policy database is compiled. If you receive an error message during policy compilation, contact Fortinet Support for assistance diagnosing and correcting the problem.

You can also create a policy database that exceeds some or all of the maximum values but can be successfully compiled. If you plan to create a configuration with one or more parameters close to or above their maximum values, you should contact Fortinet Support to review your configuration before deploying it.

It is a best practice to restart your FortiGate after making significant changes to a hyperscale policy database, especially if one or more parameters are close to or above their maximum values.

Hyperscale policy database complexity and performance

The complexity of your hyperscale firewall policy set affects how long it takes for your FortiGate to start up. In general, more complex policy databases result in longer start up times.

The complexity of your hyperscale firewall policy database also affects your FortiGate's hyperscale connections per second (CPS) performance. In general, more complex policy databases result in lower CPS performance.

How policy database changes are implemented while the FortiGate is processing traffic

The complexity of your hyperscale firewall policy database affects how long it takes after inputting a policy change before the updated policy database can be applied to new and established sessions. This period of time is called the preparation time.

During the preparation time, new sessions are evaluated with the current policy database.

After the preparation time, new sessions are evaluated with the new policy database. Established sessions are also re-evaluated with the new policy database . The time required to re-evaluate established sessions is called the transition time. CPS performance can be reduced during the transition time.

The transition time is affected by hyperscale policy database complexity, the total number of established sessions to be re-evaluated, and by the rate that the system is receiving new sessions.

During the transition time, FortiOS terminates an established session if:

- The session is matched with a policy that has a different policy search key (for example, a different source IP range)or policy action.
- The session is matched with the same policy but the policy includes a resource, such as an IP pool, that dynamically assigns a value (for example, an IP address) to the session and now it has to be returned because of the policy change.

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 6.4.10 Build 2000. The Special notices described in the FortiOS 6.4.10 release notes also apply to Hyperscale firewall for FortiOS 6.4.10 Build 2000.

Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 6.4.11, 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 port33 to port36 interfaces of the FortiGate-2600F and 2601F.
- The port31 to port36 interfaces of the FortiGate-3500F and 3501F.
- 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 6.4.11 incompatibilities and limitations

Hyperscale firewall for FortiOS 6.4.11 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 6.4.10 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, 6.4.6, 6.4.8, or 6.4.9 firmware and is licensed for hyperscale firewall features, you can follow a normal firmware upgrade process to upgrade to FortiOS 6.4.10.

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 6.4.10. Once you have upgraded to 6.4.10 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 8.

Product integration and support

The Product integration and support information described in the FortiOS 6.4.10 release notes also applies to Hyperscale firewall for FortiOS 6.4.10 Build 2000.

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 6.4.11 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 6.4.10 Build 2000. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 6.4.10 release notes also apply to Hyperscale firewall for FortiOS 6.4.10 Build 2000.

Bug ID	Description
759344 791761	NP7 CAPWAP offloading for WiFi traffic now supports VLAN-related features such as dynamic VLANs and VLAN stacking (also called QinQ or inner VLANs).
775529 724675	FortiGates with NP7 processors can now establish protocol independent multicast v2 (PIMv2) neighbors through a hardware switch interface and can also pass VRRP packets.
778794	Resolved an issue that caused DoS anomaly logs for NP7-offloaded DoS policy sessions to incorrectly report the number of times that an anomaly was detected or blocked in the repeats field of DoS anomaly log messages.
803892 801770	The `iport` and `oport` configuration of the `dsw-queue-dts-profile` option of the `config system npu` command is no lost when upgrading to FortiOS 6.4.10.
815253	Resolved an issue that could sometimes randomly block traffic in NP7-offloaded IPsec VPN tunnels. The problem would happen more often as the number of IPsec VPN tunnels increased.
821230	Resolved some issues around the use and display of the `service-negate` option when creating and editing hyperscale firewall policies.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 6.4.10 Build 2000. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 6.4.10 release notes also apply to Hyperscale firewall for FortiOS 6.4.10 Build 2000.

Bug ID	Description
724085	Traffic offloaded by NP7 processors is blocked by EMAC-VLAN interfaces when the parent interface is in another VDOM. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected.
796368	Hyperscale firewall VDOMs do not support traffic shaping policies or profiles. Only outbandwidth traffic shaping is supported for hyperscale firewall VDOMs.
802369	Hyperscale firewall policies containing a fixed allocation IP pool and a large number of client IP addresses (for example, 65K addresses) can cause high CPU usage and can reduce overall system performance.
817091	NP7 processors drop ICMP and UDP sessions in an asymmetric FGSP cluster if the sessions are accepted by a firewall policy with UTM enabled.