Hyperscale Firewall - Release Notes

Version 6.4.9 Build 1966

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 6.4.9 Build 1966 Release Notes
01-649-800782-20230111

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 6.4.9 incompatibilities and limitations on page 9.
May 3, 2022	Added information to Upgrade information on page 12 about confirming the configuration of the `dsw-queue-dts-profile` option of the `config system npu` command after upgrading to FortiOS 6.4.9.
April 26, 2022	Initial version.

Hyperscale firewall for FortiOS 6.4.9 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 6.4.9 Build 1966.

In addition, special notices, changes in the CLI, changes in default behavior, changes in table size, new features and enhancements, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 6.4.9 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 6.4.9 Build 1966.

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 6.4.9 Build 1966 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

Hyperscale firewall for FortiOS 6.4.9 Build 1966 includes the bug fixes described in Resolved issues on page 14.

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 6.4.9 Build 1966. The Special notices described in the FortiOS 6.4.9 release notes also apply to Hyperscale firewall for FortiOS 6.4.9 Build 1966.

Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 6.4.9, 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
```

Blackhole and loopback routes and BGP in a hyperscale VDOM

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

Forward error correction only available for 100 GigE interfaces

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

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

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

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

FortiGates with NP7 processors and NetFlow domain IDs

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

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

Hyperscale firewall 6.4.9 incompatibilities and limitations

Hyperscale firewall for FortiOS 6.4.9 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.
- 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 6.4.9 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.

If your FortiGate is currently running FortiOS 6.2.6, 6.2.7, 6.2.9, 6.4.6, or 6.4.8 firmware and is licensed for hyperscale firewall features, you can follow a normal firmware upgrade process to upgrade to FortiOS 6.4.9.

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 6.4.9. Once you have upgraded to 6.4.9 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 7.

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

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

When this command was first added with FortiOS 6.4.6, the `iport` and `oport` options were all uppercase. However, for 6.4.8 they were converted to lower case. This change was missed in the upgrade code, so your configuration of this command may be lost after upgrading to 6.4.9.

Product integration and support

The Product integration and support information described in the FortiOS 6.4.9 release notes also applies to Hyperscale firewall for FortiOS 6.4.9 Build 1966.

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 6.4.9 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 6.4.9 Build 1966. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 6.4.9 release notes also apply to Hyperscale firewall for FortiOS 6.4.9 Build 1966.

Bug ID	Description
757417	With per-session accounting enabled on a hyperscale firewall FGCP HA cluster, when you change the configuration of a hyperscale firewall policy that is not currently accepting traffic, the hit counter for the policy no longer increases on the secondary FortiGate.
758990 758364 760705	Resolved multiple synchronization issues between FortiGates operating as hyperscale firewall in an FGCP cluster.
759154 760787	Enabling `srcaddr-negate` in a hyperscale firewall policy now works as expected when the policy includes more than one source address.
759639 760544 771346 774481 766013 769866	Resolved multiple NP7 per-policy-accounting issues.
760785	The `config system npu` option `double-level-mcast` has been removed from the CLI because enabling this option could cause traffic flow issues.
761465	Resolved an issue that would allow sessions to pass through the FortiGate after changing the IP pool configuration of a hyperscale firewall policy to block these sessions. This was occurring because of the time delay between installing a firewall policy change in the kernel and then adding the firewall policy change to the NP7 processor hardware policy table. This issue has been partially resolved by blocking all sessions for packets that match the IP pool that has changed for a short time to allow policy changes to be made to the NP7 processor hardware policy table.
765582	Resolved an issue for FortiGates with NP7 processors that blocked traffic from passing through the FortiGate if one of the interfaces is a Vxlan interface that is part of a software switch.
768417	NAT64 and NAT46 hyperscale firewall policy names are now included in NP7 policy engine (NPD) firewall policy information.
769856	Resolved an issue that caused messages similar to `NPD WRITE CDB_ARP_HTAB_CSR FAILED, ret -1013!` to appear on the console of a FortiGate with NP7 processors. To resolve the issue, NP7 systems were upgraded to be able to handle larger numbers of ARP table entries. Related to this issue, if you use the system global CLI option `arp-max-entry` to change the maximum number of dynamically learned MAC addresses that can be added to the ARP table, a best practice is to restart your FortiGate to make sure the system adjusts the size of the ARP tables as expected.
771221	Resolved an issue that caused the time recorded by hardware syslog messages to be incorrect.

Bug ID	Description
771250	Resolved an issue that could cause a system restart after pressing **Ctrl+C** from the CLI (for example, to interrupt the output of the `diagnose npd policy dump` command).
771875	Resolved an issue that blocked NP7 offloaded TFTP sessions after an FGCP HA failover.
772394	The `lookup` option of the `diagnose npd policy` command has been removed.
774186	Resolved an issue that caused hardware sessions synchronized by FGSP for a hyperscale fireweall VDOM to be synchronized in software instead of being handled by NP7 processors.
774862	Resolved an issue that could cause traffic to be blocked after changing the destination address in a hyperscale firewall policy from a firewall virtual IP to a normal firewall address.
783410	Resolved an issue with how the NP7 policy engine (NPD) interprets IPv6 firewall addresses that caused the npd to accept traffic with IPv6 addresses that were outsideof the subnet specified in the firewall address.
797993 766661	Resolved an issue that could cause issues such as blocked sessions or traffic shaping settings not taking affect when outbound traffic shaping is applied to sessions that are offloaded to NP7 processors by NTurbo.
792875	Resolved issues with multicast logging that could cause FortiGates in an FGCP HA cluster to restart after changing the HA priority.
800316	Resolved an issue that prevented NP7 processors from offloading CAPWAP traffic.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 6.4.9 Build 1966. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 6.4.9 release notes also apply to Hyperscale firewall for FortiOS 6.4.9 Build 1966.

Bug ID	Description
796368	Hyperscale firewall VDOMs do not support traffic shaping policies or profiles. Only outbandwidth traffic shaping is supported for hyperscale firewall VDOMs.
756537	Some FortiView Session GUI pages allow you to select options to display some Hyperscale sessions, even though hardware session information is not available to FortiView.
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.