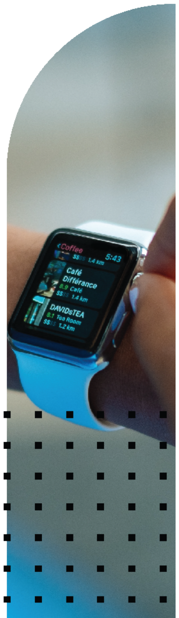
Release Notes

Hyperscale Firewall 7.0.9 Build 0444



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®

March 15, 2023
Hyperscale Firewall 7.0.9 Build 0444 Release Notes
01-709-861761-20230315

TABLE OF CONTENTS

Change log

Date	Change description
March 15, 2023	Removed known issue 782674, which was resolved in a previous version of FortiOS.
January 11, 2023	Added more information about `arp-reply` support limitations for IPv4 and IPv6 firewall VIPs to Hyperscale firewall 7.0.9 incompatibilities and limitations on page 9.
November 22, 2022	Initial version.

Hyperscale firewall for FortiOS 7.0.9 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 7.0.9 Build 0444.

In addition, special notices, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 7.0.9 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 7.0.9 Build 0444.

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 7.0.9 Build 0444 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
- FortiGate-3501F
- FortiGate-4200F
- FortiGate-4201F
- FortiGate-4400F
- FortiGate-4401F

What’s new

Hyperscale firewall for FortiOS 7.0.9 Build 0444 includes the bug fixes described in Resolved issues.

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 7.0.9 Build 0444. The Special notices described in the FortiOS 7.0.9 release notes also apply to Hyperscale firewall for FortiOS 7.0.9 Build 0444.

Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 7.0.9, 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 forward to the CPU and these settings should not be changed.

If you want a BGP route entry regardless of whether there is a real route or not, you can use the BGP `network-import-check` option to determine whether a network prefix is advertised or not. For more information, see Allow per-prefix network import checking in BGP.

Forward error correction only available for 25 and 100 GigE interfaces

On FortiGate models with NP7 processors, the `forward-error-correction` CLI option is only available for interfaces with `speed` set to `25000full`, `25000auto`, `100Gfull` or `100Gauto`. Forward error connection is not supported for interfaces in FortiGates with NP7 processors when the interface is configured to operate at any other speed.

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 7.0.9 incompatibilities and limitations

Hyperscale firewall for FortiOS 7.0.9 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 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 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 7.0.9 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, 6.4.8, 6.4.9, 7.0.5, 7.0.6, 7.0.7, or 7.0.8 firmware and is licensed for hyperscale firewall features, you can follow a normal firmware upgrade process to upgrade to FortiOS 7.0.9.

If you are currently operating a FortiGate with NP7 processors without a hyperscale firewall license, you can use the upgrade path to upgrade to FortiOS 7.0.9. Once you have upgraded to 7.0.9 you can activate your hyperscale firewall license and set up your hyperscale firewall configuration.

The firmware upgrade code does not support upgrading NAT64 and NAT46 firewall policies or VIP46 and VIP64 firewall policies to 7.0.9. After upgrading, you should review all NAT64 and NAT46 firewall policies and all VIP64 and VIP46 firewall policies added prior to upgrading.

In FortiOS 7.0.9, you apply hyperscale firewall features by creating normal firewall policies in hyperscale firewall VDOMs. FortiOS 7.0.9 no longer has hyperscale firewall policies in a separate hyperscale firewall policy list, as supported by FortiOS 6.2 and 6.4.

The FortiOS 7.0.9 upgrade process converts FortiOS 6.2 and 6.4 hyperscale firewall policies to normal firewall policies and adds them to the normal policy list in their hyperscale firewall VDOMs. During the conversion process, the policy IDs of the hyperscale firewall policies may be changed when they are converted to normal firewall policies.

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.

Product integration and support

This section describes Hyperscale firewall for FortiOS 7.0.9 Build 0444 product integration and support information. The Product integration and support information described in the FortiOS 7.0.9 release notes also applies to Hyperscale firewall for FortiOS 7.0.9 Build 0444.

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

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 7.0.9 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 7.0.9 Build 0444. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 7.0.9 release notes also apply to Hyperscale firewall for FortiOS 7.0.9 Build 0444.

Bug ID	Description
837095	Resolved an issue with how the `wad` process handles CA certificates that caused the `wad` process to use excessive amounts of CPU time with many child processes after creating 250 hyperscale firewall VDOMs.
848938	Resolved an issue that could cause the Session Search Engine (SSE) running on an NP7 processor on the primary FortiGate in an FGCP cluster to stop working after receiving an HASYNC message from the secondary FortiGate.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 7.0.9 Build 0444. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 7.0.9 release notes also apply to Hyperscale firewall for FortiOS 7.0.9 Build 0444.

Bug ID	Description
724085	Traffic passing through an EMAC-VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If you set the `auto-asic-offload` option to `disable` in the firewall policy, traffic flows as expected.
763966	FGSP synchronizes NP7 sessions from all VDOMs when FGSP is configured to synchronize sessions from a hyperscale VDOM.
795853	Disabling EIF and EIM in a hyperscale firewall policy actively processing traffic causes errors in the information stored in the NP7 firewall policy database. For example, the data may include incorrect VDOM IDs and IP addresses.
807476	On a FortiGate licensed for Hyperscale firewall features, using the `cfg-save` option of the `config system global` command to revert configuration changes may result in error messages displaying on the CLI. The error occurs because when packets go through host interface TX/RX queues, some packet buffers can still hold references to VDOM when the host queues are idle. If more packets go through the same host queues for other VDOMs, the issue should resolve.
810225	On FortiGates with NP7 processors, the first time you change the password of a newly created administrator fro the GUI an "undefined" error message may appear.
811109	The HA1, HA2, AUX1, and AUX2 interfaces of the FortiGate-4200F, 4201F, 4400F, and 4401F cannot be added to a LAG.
836976	Sessions being processed by hyperscale firewall policies with hardware logging may be dropped when dynamically changing the log server `log-processor` mode from `hardware` to `host` for the hardware log sever added to the hyperscale firewall policy. To avoid dropping sessions, change the log-processor setting during quiet periods.
838654	In a hyperscale firewall VDOM, NAT64 and NAT46 sessions offloaded to NP7 processors that are blocked by the implicit deny policy do not increase the implicit deny policy hit count.
839958	The `service-negate` firewall policy option does not work as expected in a hyperscale deny policy.
841712	The `config system npu` option `nat64-force-ipv4-packet-forwarding` is not available.
842008	If background session scanning is enabled (using the `background-sse-scan` option of the `config system npu` command, after an FGCP HA failover, some sessions may not be synchronized from the primary to the secondary FortiGate.
842659	The `srcaddr-negate` and `dstaddr-negate` options do not work as expected for IPv6 FTS traffic.

Bug ID	Description
843132	Access control list (ACL) policies added while a FortiGate is processing traffic may take longer than expected to become effective. During a transition period, traffic that should be blocked by the ACL policy will be allowed.
843197	The output of the `diagnose sys npu-session list/list-full` command does not include policy route information.
843266	Hyperscale firewall sessions that are routed by policy routes do not show information such as hit count and last used when displayed with the `diagnose firewall proute list` command.
843305	A message similar to PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS can appear on the console error log when a FortiGate with NP7 processors starts up.
844421	Due to a hardware limitation, when overload mode IP pools are used, the per IP pool session stats are not accurate.
846520	After an FGCP HA failover, the NPD/LPMD processes may be stopped by an out of memory killer process after running mixed sessions even when the amount of memory use is not excessive.
847314	FortiGates with NP7 processors may encounter random kernel crashes after a system restart or a factory reset.
847664	FortiGates with NP7 processors may display an error message similar to `mce: [Hardware Error]` while starting up.

www.fortinet.com