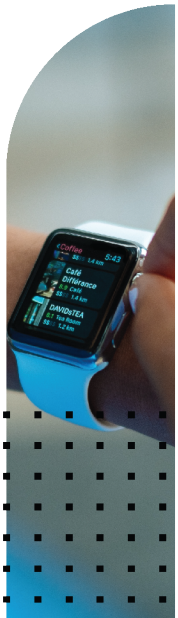
Release Notes

Hyperscale Firewall 7.0.5 Build 4515



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

March 16, 2023
Hyperscale Firewall 7.0.5 Build 4515 Release Notes
01-705-780810-20230316

TABLE OF CONTENTS

Change log

Date	Change description
March 16, 2023	Removed 782674 from Resolved issues on page 14. This known issue was resolved in FortiOS 7.0.8.
January 11, 2023	Added more information about `arp-reply` support limitations for IPv4 and IPv6 firewall VIPs to Hyperscale firewall 7.0.5 incompatibilities and limitations on page 9.
November 17, 2022	Add the FortiGate-3000F and 3001F to Supported FortiGate models on page 5.
September 28, 2022	FortiOS 7.0.5 Hyperscale firewall VDOMs support consolidated firewall policies. The statement about Hyperscale firewall VDOMs not supporting consolidated firewall policies has been removed from Hyperscale firewall 7.0.5 incompatibilities and limitations on page 9.
June 15, 2022	Added information about how FortiOS 7.0.5 hyperscale policies are no longer separated from normal firewall policies and how hyperscale firewall policies are converted during the upgrade process to Upgrade information on page 12.
June 8, 2022	Fixed some broken links.
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.
March 4, 2022	Initial version.

Hyperscale firewall for FortiOS 7.0.5 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 7.0.5 Build 4515.

In addition, special notices, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 7.0.5 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 7.0.5 Build 4515.

Since this is the first NP7 and Hyperscale firewall release supported by FortiOS 7.0, this release is also the first time FortiOS 7.0 features are available for NP7 processors and for FortiGates that support Hyperscale firewall features.

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 7.0.5 Build 4515 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-3000F
- FortiGate-3001F
- FortiGate-3500F
- FortiGate-3501F
- FortiGate-4200F
- FortiGate-4201F
- FortiGate-4400F
- FortiGate-4401F

What's new

The following new features have been added to Hyperscale firewall for FortiOS 7.0.5 Build 4515.

NP7 hardware logging supports multicast logging

You can now configure NP7 hardware logging to support multicast logging. Previous hyperscale firewall versions of FortiOS only supported multicast logging for CPU or host logging.

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

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

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

Set `log-tx-mode` to `multicast` to simultaneously send session setup log messages to multiple remote syslog or NetFlow servers.

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 7.0.5 Build 4515. The Special notices described in the FortiOS 7.0.5 release notes also apply to Hyperscale firewall for FortiOS 7.0.5 Build 4515.

Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 7.0.5, 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 7.0.5 incompatibilities and limitations

Hyperscale firewall for FortiOS 7.0.5 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 7.0.5 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 7.0.5.

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 7.0.5. Once you have upgraded to 7.0.5 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 7.0.5. After upgrading, you should review all NAT64 and NAT46 firewall policies and all VIP64 and VIP46 firewall policies added prior to upgrading.

In FortiOS 7.0.5, you apply hyperscale firewall features by creating normal firewall policies in hyperscale firewall VDOMs. FortiOS 7.0.5 no longer has hyperscale firewall policies in a separate hyperscale firewall policy list, as supported by FortiOS 6.2 and 6.4.

The FortiOS 7.0.5 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.

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 7.0.5.

Product integration and support

This section describes Hyperscale firewall for FortiOS 7.0.5 Build 4515 product integration and support information. The Product integration and support information described in the FortiOS 7.0.5 release notes also applies to Hyperscale firewall for FortiOS 7.0.5 Build 4515.

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

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 7.0.5 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 7.0.5 Build 4515. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 7.0.5 release notes also apply to Hyperscale firewall for FortiOS 7.0.5 Build 4515.

Bug ID	Description
780315	Resolved an issue that reduces connections per second (CPS) performance for VLAN traffic.
780160	Resolved an issue that can cause a PBA leak when running multiple npu sniffers at the same time.
769556 781275 786699	NP7 nTurbo support for offloaded GRE and IPIP tunnels now works as expected.
781653	NP7 offloading of IPv6 tunnels now works as expected.
784010	NP7 offloading of IP SIT tunnels now works as expected.
781449	Resolved an issue that caused sessions to be dropped or extra sessions to be created in a hyperscale firewall VDOM when making changes to firewall policies while the hyperscale firewall VDOM is actively processing traffic.
784181	In a hyperscale firewall VDOM, changes to the firewall policies stored in the NP7 processor firewall policy table are now correctly synchronized to the software copy of the firewall policy table.
778052	Resolved an issue that prevented synchronizing software sessions to the secondary FortiGate in an HA cluster after the primary FortiGate fails and is restored to operating as the primary FortiGate.
779314	Resolved an issue that blocked traffic through hairpin configurations involving IPv4 NAT or NAT64 traffic.
788615	Resolved an issue that caused RLT packets to be lost when processing traffic with jumbo frames.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 7.0.5 Build 4515. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 7.0.5 release notes also apply to Hyperscale firewall for FortiOS 7.0.5 Build 4515.

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.
775529 724675	FortiGates with NP7 processors cannot establish protocol independent multicast v2 (PIMv2) neighbors through a hardware switch interface and also cannot pass VRRP packets.
752024	Hyperscale firewall hardware traffic logs do not include the action field and do not indicate whether the policy action is allow or deny.
766494	In a hyperscale firewall VDOM, fixed port range NAT does not match all of the behavior for deterministic NAT as described in RFC 7422.
767232	Configuring the `in-bandwidth` interface option for a tunnel interface does limit traffic flow through the tunnel interface.
773221	IPsec traffic that passes through a loopback interface cannot be offloaded by NP7 processors.
774260	You may notice that excessive numbers of packets are lost through IPSec tunnels with AES256-GCM encryption.
777212	Hardware logging log messages are not created for firewall policies with action set to deny.
781302	You cannot change the address type of an IPv6 firewall address that has been added to a firewall address group.
782127	Traffic is blocked by NAT64 and NAT46 policies when `src-negate` is enabled.
782674	On the secondary FortiGate in an FGCP cluster, the `diagnose sys npu-sessions st verbose` command output shows hung tasks when an FGCP cluster is processing a large number of sessions. These messages only appear on the secondary FortiGate.
783611	Incorrect information provided by the `fgFwHsPolLastUsed` MIB field.
783649	Incorrect information provided by the `fgSysNpuSes6Count` MIB field.
787344	SIP sessions that match NAT64 hyperscale firewall policies are blocked.
787864	The `diagnose sys npu-session clear` command when used with the hardware session filter does not clear all of the sessions that should be cleared.
787888	With hardware logging set to CPU logging (or host logging), FortiView session pages don't show any data in the Source interface, Destination interface, Packets, and Bytes columns.

Bug ID	Description
788703	In an FGCP cluster, trap sessions are not tagged as NP7 offloaded sessions in the secondary FortiGate session table.
788836	IPv6 DTLS IPsec VPN wireless traffic is blocked when NP7 CAPWAP offloading is enabled.
790267	When creating a NAT64 firewall policy in a hyperscale VDOM, you cannot select IP pools to add to the policy.
791335	Hardware logging log messages do not include information about logged in SSO or RSSO users.
793135	Schedules and security profiles cannot be added to hyperscale firewall policies. However, when creating or editing a firewall policy in a hyperscale firewall VDOM from the GUI the schedule option may be visible, but you can't use it to select a schedule. Also, some GUI pages that display firewall policy information may incorrectly include the schedule and security profile fields.
793545	In hyperscale firewall VDOMs, the IP Pools Utilization and Top IP Pools by Assigned IPs widgets that appear on the **Firewall > IP Pools** GUI page do not show any results.
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.
795990	Miscellaneous traffic drops, slow downs, and memory leaks found for ARP and RLT and others.

www.fortinet.com