FORTINET

Release Notes

Hyperscale Firewall 7.2.1 Build 1254

January 10, 2023
Hyperscale Firewall 7.2.1 Build 1254 Release Notes
01-721-830237-20230110

TABLE OF CONTENTS

Change log

Date	Change description
January 10, 2023	Added more information about `arp-reply` support limitations for IPv4 and IPv6 firewall VIPs to Hyperscale firewall 7.2.1 incompatibilities and limitations on page 12.
September 28, 2022	FortiOS 7.2.1 Hyperscale firewall VDOMs support consolidated firewall policies. The statement about Hyperscale firewall VDOMs not supporting consolidated firewall policies has been removed from Hyperscale firewall 7.2.1 incompatibilities and limitations on page 12.
August 17, 2022	New feature added, see FGSP HA hardware session synchronization on page 6 and Basic FGSP HA hardware session synchronization configuration example on page 6. Changes to Hyperscale firewall 7.2.1 incompatibilities and limitations on page 12 to reflect that FortiOS 7.2.1 supports FGSP HA hardware session synchronization. Changes to Optimizing FGCP HA hardware session synchronization with data interface LAGs on page 8 and Recommended interface use for an FGCP HA hyperscale firewall cluster on page 8.
August 4, 2022	Changes to Recommended interface use for an FGCP HA hyperscale firewall cluster on page 8. Known issue 824071 added to Known issues on page 17.
August 4, 2022	Initial version. New sections: • Recommended interface use for an FGCP HA hyperscale firewall cluster on page 8. • Optimizing FGCP HA hardware session synchronization with data interface LAGs on page 8.

Hyperscale firewall for FortiOS 7.2.1 release notes

These platform specific release notes describe special notices, upgrade information, product integration and support, resolved issues, and known issues for FortGates licensed for Hyperscale firewall features for FortiOS 7.2.1 Build 1254.

In addition, special notices, changes in CLI, changed in default behavior, new features and enhancements, upgrade information, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 7.2.1 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 7.2.1 Build 1254.

Since this is the first NP7 and Hyperscale firewall release supported by FortiOS 7.2, this release is also the first time FortiOS 7.2 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 7.2.1 Build 1254 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

The following new features have been added to Hyperscale firewall for FortiOS 7.2.1 Build 1254. The changes in the CLI, changes in GUI behavior, changes in default behavior, and new features or enhancements described in the FortiOS 7.2.1 release notes also apply to Hyperscale firewall for FortiOS 7.2.1 Build 1254.

FGSP HA hardware session synchronization

When configuring FortiGate Session Life Support Protocol (FGSP) clustering for two hyperscale firewall FortiGate peers, you can use FGSP HA hardware session synchronization to synchronize NP7 hyperscale firewall sessions between the FortiGate peers in the cluster. The FortiGate peers can be:

- Two FortiGates
- Two FGCP clusters
- One FortiGate and one FCGP cluster

Configuring the HA `hw-session-sync-dev` option is not required for FGSP HA hardware session synchronization. Instead, you set up a normal FGSP configuration for your hyperscale firewall VDOMs and use a data interface or data interface LAG as the FGSP session synchronization interface. The data interface can be a physical interface or a VLAN.

Select a data interface or create a data interface LAG for FGSP HA hardware session synchronization that can handle the expected traffic load. For example, from Fortinet's testing, hyperscale rates of 4,000,000 connections per second (CPS) can use 35Gbps of data for FGSP HA hardware session synchronization. If the CPS rate is higher, FGSP HA hardware session synchronization data use may spike above 50Gbps.

FGSP HA hardware session synchronization packets are distributed by the internal switch fabric to the NP7 processors just like normal data traffic. If you create a data interface LAG for FGSP HA hardware session synchronization, no special configuration of the data interface LAG is required for optimal performance.

FGSP HA hardware session synchronization does not support session filters (configured with the `config session-sync-filter option`).

For more information about FGSP, see FGSP.

Just like any FGSP configuration, the FortiGates must be the same model. The configurations of the hyperscale VDOMs on each FortiGate must also be the same. This includes VDOM names, interface names, and firewall policy configurations. You can use configuration synchronization to synchronize the configurations of the FortiGates in the FGSP cluster (see Standalone configuration synchronization). You can also configure the FortiGate separately or use FortiManager to keep key parts of the configuration, such as firewall policies, synchronized

Basic FGSP HA hardware session synchronization configuration example

The following steps describe how to set up a basic FGSP configuration to provide FGSP HA hardware session synchronization between one or more hyperscale firewall VDOMs in two FortiGate peers.

Use the following steps to configure FGSP on both of the peers in the FGSP cluster.

1. Enable FGSP for a hyperscale firewall VDOM, named MyCGN-hw12:

   ```
   config system standalone-cluster
     config cluster-peer
       edit 1
         set peerip 1.1.1.1
         set syncvd MyCGN-hw12
       end
   ```

   If your FortiGate has multiple hyperscale firewall VDOMs, you can add the names of the hyperscale VDOMs to be synchronized to the `syncvd` option. For example:

   ```
   config system standalone-cluster
     config cluster-peer
       edit 1
         set peerip 1.1.1.1
         set syncvd MyCGN-hw12, MyCGN-hw22
       end
   ```

   In most cases you should create only one cluster-sync instance. If you create multiple cluster-sync instances, all FGSP HA hardware session synchronization sessions will be sent to the interface used by each cluster-sync instance.

2. Configure FGSP session synchronization as required. All session synchronization options are supported. For example:

   ```
   config system ha
     set session-pickup enable
     set session-pickup-connectionless enable
     set session-pickup-expectation enable
     set session-pickup-nat enable
   end
   ```

3. Configure networking on the FortiGate so that traffic to be forwarded to the peer IP address (in the example, 1.1.1.1) passes through a data interface or data interface LAG.

   This data interface or data interface LAG becomes the FGSP HA hardware session synchronization interface. If the data interface or data interface LAG is in the root VDOM, no additional configuration is required.

   If the data interface or data interface LAG is not in the root VDOM, you need to use the `peervd` option to specify the VDOM that the interface is in. For example, if the data interface or data interface LAG is in the MyCGN-hw12 VDOM:

   ```
   config system standalone-cluster
     config cluster-peer
       edit 1
         set peerip 1.1.1.1
         set syncvd MyCGN-hw12, MyCGN-hw22
         set peervd MyCGN-hw12
     end
   ```

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 7.2.1 Build 1254. The Special notices described in the FortiOS 7.2.1 release notes also apply to Hyperscale firewall for FortiOS 7.2.1 Build 1254.

Optimizing FGCP HA hardware session synchronization with data interface LAGs

The information in this section applies to FGCP HA hardware session synchronization only. FGSP HA hardware session synchronization packets are distributed by the internal switch fabric to the NP7 processors just like normal data traffic.

For optimal performance, the number of interfaces in the data interface LAG used for FGCP HA hardware session synchronization should divide evenly into the number of NP7 processors. This will distribute FGCP HA hardware session synchronization traffic evenly among the NP7 processors.

For example, the FortiGate-4200F has four NP7 processors. For optimum performance, the data interface LAG used for FGCP HA hardware session synchronization should include four or eight data interfaces. This configuration distributes the hardware session synchronization sessions evenly among the NP7 processors.

For a FortiGate-4400F with six NP7 processors, the optimal data interface LAG would include six or twelve data interfaces.

For a FortiGate-3500F with three NP7 processors, the optimal data interface LAG would include three or six data interfaces.

LAGs with fewer interfaces than the number of NP7 processors will also distribute sessions evenly among the NP7 processors as long as the number of data interfaces in the LAG divides evenly into the number of NP7 processors.

For best results, all of the data interfaces in the LAG should be the same type and configured to operate at the same speed. You can experiment with expected traffic levels when selecting the number and speed of the interfaces to add the LAG. For example, if you expect to have a large amount of hardware session synchronization interface traffic, you can add more data interfaces to the LAG or use 25G instead of 10G interfaces for the LAG.

Recommended interface use for an FGCP HA hyperscale firewall cluster

When setting up an FGCP HA cluster of two FortiGates operating as hyperscale firewalls, you need to select interfaces to use for some or all of the following features:

- Management.
- HA heartbeat (also called HA CPU heartbeat).
- HA session synchronization (also called HA CPU session synchronization).
- FGCP HA hardware session synchronization.
- Hardware logging.
- CPU logging.
- Logging to FortiAnalyzer

The following table contains Fortinet's recommendations for the FortiGate interfaces to use to support these features.

Interfaces	Recommended for
MGMT1 and MGMT2	Normal management communication with the FortiGates in the cluster.
HA1 and HA2	HA heartbeat (also called HA CPU heartbeat) between the FortiGates in the cluster.
AUX1 and AUX2	HA session synchronization (also called HA CPU session synchronization) or session pickup. The AUX1 and AUX2 interfaces are available only on the FortiGate 4200F/4201F and 4400F/4401F. For other FortiGate models, you can use any available interface or LAG for HA CPU session synchronization. For example, you may be able to use the HA1 and HA2 interfaces for both HA CPU heartbeat and HA CPU session synchronization. If you need to separate HA CPU heartbeat traffic from HA CPU session synchronization traffic, you can use a data interface or a data interface LAG for HA CPU session synchronization.
Data interface or data interface LAG	FGCP HA hardware session synchronization. If you use a data interface LAG as the FGCP HA hardware session synchronization interface, the LAG cannot be monitored by HA interface monitoring.
Data interface or data interface LAG	Hardware logging, CPU logging, and logging to a FortiAnalyzer. Depending on bandwidth use, you can use the same data interface or data interface LAG for all of these features.

Check the NP queue priority configuration after a firmware upgrade

After upgrading your FortiGate with NP7 processors to 7.2.1, 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 7.2.1 incompatibilities and limitations

Hyperscale firewall for FortiOS 7.2.1 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 does not support HA hardware session synchronization. Active-passive FGCP HA, FGSP, and virtual clustering do support 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 7.2.1 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, or 7.0.6 firmware and is licensed for hyperscale firewall features, you can follow a normal firmware upgrade process to upgrade to FortiOS 7.2.1.

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 7.2.1. Once you have upgraded to 7.2.1 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 7.2.1. After upgrading, you should review all NAT64 and NAT46 firewall policies and all VIP64 and VIP46 firewall policies added prior to upgrading.

In FortiOS 7.2.1, you apply hyperscale firewall features by creating normal firewall policies in hyperscale firewall VDOMs. FortiOS 7.2.1 no longer has hyperscale firewall policies in a separate hyperscale firewall policy list, as supported by FortiOS 6.2 and 6.4.

The FortiOS 7.2.1 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 9.

Product integration and support

The Product integration and support information described in the FortiOS 7.2.1 release notes also applies to Hyperscale firewall for FortiOS 7.2.1 Build 1254.

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 7.2.1 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 7.2.1 Build 1254. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 7.2.1 release notes also apply to Hyperscale firewall for FortiOS 7.2.1 Build 1254.

Bug ID	Description
805808	Resolved an issue on FortiGates with NP7 processors that could cause TCP packets to be dropped because of how packet fragmenting was handled for sessions with proxy inspection and antivirus.
810025	EIF now supports hairpinning for NAT64 sessions.
812844	Multiple default routes are now handled as expected by Hyperscale firewall VDOMs.
818811	Resolved an issue with NTurbo that caused FortiGates with NP7 processors to crash when offloading SSL mirror traffic to NP7 processors.
821799	Resolved an issue with how NP6 and NP7 processors handle IPsec VPN ID with IPIP encapsulation tunnels. This issue could cause traffic failure for IPsec VPN tunnels between two FortiGates that are both using NP6 or NP7 processors to offload the IPsec VPN traffic. This problem would only occur when VPN ID with IPIP encapsulation causes the NP6 or NP7 processor to perform pre-IPsec packet fragmentation.
825622	In a Hyperscale firewall VDOM, you can no longer change the CGN IP pool type to be incompatible with the IP pool configuration. In previous releases, it was possible that changing to an CGN IP pool type that is not compatible with the configuration of the IP pool would cause the `npd` process to crash and possibly restart the FortiGate.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 7.2.1 Build 1254. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 7.2.1 release notes also apply to Hyperscale firewall for FortiOS 7.2.1 Build 1254.

Bug ID	Description
804742	After changing hyperscale firewall policies, it may take longer than expected for the policy changes to be applied to traffic. The delay occurs because the hyperscale firewall policy engine enhancements added to FortiOS 7.2.1 may cause the FortiGate to take extra time to compile firewall policy changes and generate a new policy set that can be applied to traffic by NP7 processors. The delay is affected by hyperscale policy set complexity, the total number of established sessions to be re-evaluated, and the rate of receiving new sessions.
824733	On a FortiGate licensed for Hyperscale firewall features, IPv6 static routes may continue to be active in VDOMs after they have been deleted from the configuration. You can work around this issue by restarting the FortiGate after deleting or changing IPv6 static routes.
829549	Software ALG sessions can incorrectly add DSE entries to the NP7 session table. Traffic accepted by hyperscale firewall policies with `cgn-eif` enabled can then be matched with the DSE sessions and pass through the FortiGate.
824071	In a Multi-VDOM configuration, ECMP load balancing does not work for IPv4 and IPv6 UDP traffic passing through physical or inter-VDOM link interfaces. Instead, all UDP traffic follows the same route. ECMP load balancing of TCP traffic works as expected.

FORTINET®

www.fortinet.com