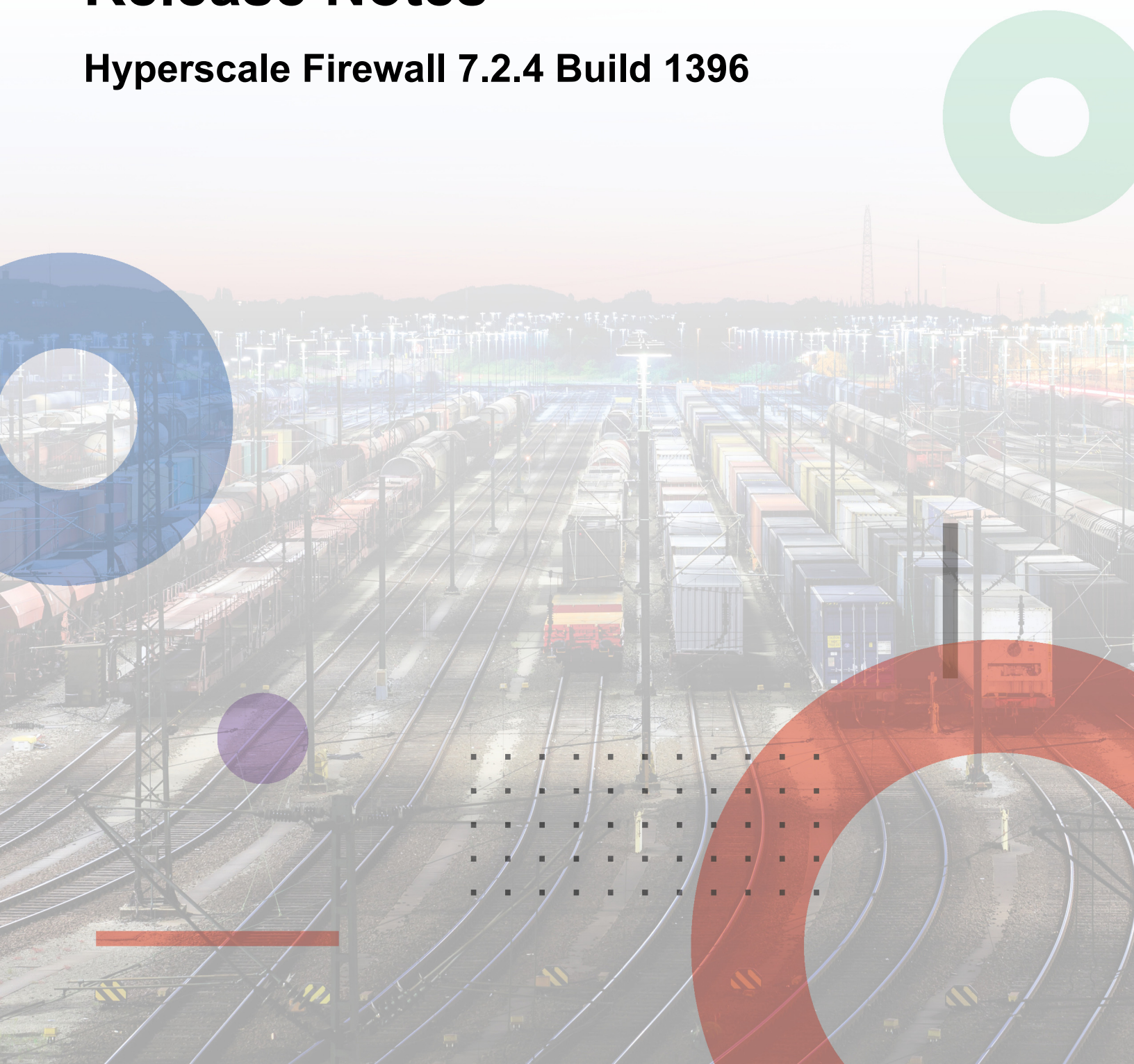
FORTINET

Release Notes

Hyperscale Firewall 7.2.4 Build 1396



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

FORTINET TRAINING 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

June 27, 2023
Hyperscale Firewall 7.2.4 Build 1396 Release Notes
01-724-873136-20230627

TABLE OF CONTENTS

Change log

Date	Change description
June 27, 2023	Added information about hardware logging sending multiple session start log messages if `log-processor` is set to `hardware` and `log-mode` is set to `per-session` to Hyperscale firewall 7.2.4 incompatibilities and limitations on page 14.
January 31, 2023	Initial version.

Hyperscale firewall for FortiOS 7.2.4 release notes

These platform specific release notes describe new features, changes in CLI, special notices, upgrade information, product integration and support, resolved issues, and known issues for FortGates licensed for Hyperscale firewall features for FortiOS 7.2.4 Build 1396.

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 7.2.4 Build 1396 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 7.2.4 Build 1396. The changes in CLI, changes in GUI behavior, changes in default behavior, changes in default values, and new features or enhancements described in the FortiOS 7.2.4 release notes also apply to Hyperscale firewall for FortiOS 7.2.4 Build 1396.

Excluding IP addresses from CGN resource allocation IP pools

You can use the new `exclude-ip` CGN resource allocation IP pool option to block a CGN IP pool from allocating one or more source IP addresses. You may want to exclude an IP address from being allocated by a CGN IP pool if the IP pool could assign an address that has been targeted by external attackers.

Exclude individual IP addresses by adding them to the CGN IP pool using the `exclude-ip` option, for example:

```
config firewall ippool
   edit <name>
      set type cgn-resource-allocation
      set exclude-ip <ip_address>, <ip_address>, <ip_address> ...
   end
```

where `<ip-address>` is a single IP address. You can only add single IP addresses. You cannot add IP address ranges. Use the ? to see how many IP addresses you can add. The limit depends on the FortiGate model.

You can't exclude IP addresses in a fixed allocation CGN resource allocation IP pool. If `cgn-fixedalloc` is set to `enable`, the `exclude-ip` option is not available.

New FGCP HA hardware session synchronization timers

Hyperscale firewall for FortiOS 7.2.4 supports the following new CLI options to set timers associated with hardware session synchronization after an FGCP HA failover:

```
config system ha
   set hw-session-sync-dev <interface-name>
   set hw-session-hold-time <seconds>
   set hw-session-sync-delay <seconds>
end
```

`hw-session-hold-time` the amount of time in seconds after a failover to hold hardware sessions before purging them from the new secondary FortiGate. The range is 0 to 180 seconds. The default is 10 seconds.

`hw-session-sync-delay` the amount of time to wait after a failover before the new primary FortiGate synchronizes hardware sessions to the new secondary FortiGate. The range is 0 - 3600 seconds. The default is 150 seconds.

After an HA failover, the new secondary FortiGate waits for the `hw-session-hold-time` and then purges all sessions and frees up all resources. Then, after the `hw-session-sync-delay`, the new primary FortiGate synchronizes all hardware sessions to the new secondary FortiGate. The `hw-session-sync-delay` gives the new secondary FortiGate enough time to finish purging sessions and freeing up resources before starting session synchronization.

The default configuration means that there is a 150 second delay before sessions are synchronized to the new secondary FortiGate. You can use the new options to adjust the timers depending on the requirements of your network conditions. For example, if you would rather not wait 150 seconds for hardware sessions to be synchronized to the new secondary FortiGate, you can adjust the `hw-session-sync-delay` timer.

Diagnose command improvements

FortiOS 7.2.4 includes the following diagnose commands that you can use to view summary information about IPv4 and IPv6 sessions offloaded to NP7 processors:

```
diagnose sys npu-session list-brief [{44 | 46}]
diagnose sys npu-session list-brief6 [{66 | 64}]
```

The command output includes lists of sessions organized by session type and a total number of sessions for each session type. Summary information for each session includes the protocol, expiry time, source and destination addresses, and source and destination NAT addresses.

New filters have been added to the `diagnose sys npu-session filter6` command to support filtering for IP addresses and ports added by source NAT for public traffic.

- `nat64_pub_ip` filter sessions based on public source IP address.
- `nat64_pub_port` filter sessions based on public source port number.

Hardware session synchronization LAGs must be static

FortiOS 7.2.4 only allows you to use a static mode LAG as the hardware session synchronization interface.

Example LAG configuration:

```
config system interface
   edit HA-session-lag
      set type aggregate
      set lacp-mode static
      set member port13 port14 port15 port16
   end
```

Example HA configuration:

```
config system ha
   set session-pickup enable
   set hw-session-sync-dev HA-session-lag
end
```

You can only add a LAG with `lacp-mode` set to `static` as the `hw-session-sync-dev` and the CLI blocks you from changing the `lacp-mode` of the `hw-session-sync-dev` LAG to `dynamic` or `passive`.

More support for hyperscale firewall polices that block sessions

FortiOS 7.2.4 supports the following new features related to hyperscale firewall policies that block sessions, that is hyperscale firewall policies with action set to deny:

- You can now enable hardware logging for hyperscale firewall policies with action set to deny. Hardware logging creates a log message for each session that is blocked.
- Hardware session information now includes information about whether the session blocked traffic. For example, when displaying session information from the CLI, a field similar to the following appears to indicate that the session blocked traffic: `Session action (DROP/TO-HOST): DROP`.

Hardware log messages now indicate if the session accepted or denied traffic. For example:

- Example log messages for a policy that accepts traffic:

  ```
  Oct 5 23:29:33 172.16.200.26 date=2022-10-06 time=02:29:32 sn=F2K61FTK21900840
  vd=cgn-hw1 pid=805306369 type=sess act=start tran=snat proto=6 ipold=v4 ipnew=v4
  sip=10.1.100.11 dip=172.16.200.155 sport=40836 dport=80 nsip=172.16.201.182
  ndip=172.16.200.155 nsport=8117 ndport=80 sentp=0 sentb=0 rcvdp=0 rcvdb=0
  Oct 5 23:29:36 172.16.200.26 date=2022-10-06 time=02:29:35 sn=F2K61FTK21900840
  vd=cgn-hw1 pid=805306369 type=sess act=end tran=snat proto=6 ipold=v4 ipnew=v4
  sip=10.1.100.11 dip=172.16.200.155 sport=40836 dport=80 nsip=172.16.201.182
  ndip=172.16.200.155 nsport=8117 ndport=80 dur=2936 sentp=6 sentb=398 rcvdp=4
  rcvdb=1307
  ```

  Decimal version of the pid = 805306369

  Binary version of the pid = 0**0**11 0000 0000 0000 0000 0000 0000 0001

  pid[30] is '**0**' for accept action (count from bit0 to bit31 and right to left)
- Example log messages for a policy that blocks or denies traffic:

  ```
  Oct 5 23:31:49 172.16.200.26 date=2022-10-06 time=02:31:49 sn=F2K61FTK21900840
  vd=cgn-hw1 pid=1946157057 type=sess act=start tran=none proto=6 ipold=v4 ipnew=v4
  sip=10.1.100.11 dip=172.16.200.155 sport=40837 dport=80 nsip=10.1.100.11
  ndip=172.16.200.155 nsport=40837 ndport=80 sentp=0 sentb=0 rcvdp=0 rcvdb=0
  Oct 5 23:32:02 172.16.200.26 date=2022-10-06 time=02:32:01 sn=F2K61FTK21900840
  vd=cgn-hw1 pid=1946157057 type=sess act=end tran=none proto=6 ipold=v4 ipnew=v4
  sip=10.1.100.11 dip=172.16.200.155 sport=40837 dport=80 nsip=10.1.100.11
  ndip=172.16.200.155 nsport=40837 ndport=80 dur=12719 sentp=2 sentb=120 rcvdp=0
  rcvdb=0
  ```

  Decimal version of the pid = 1946157057

  Binary version of the pid = 0**1**11 0100 0000 0000 0000 0000 0000 0001

  pid[30] is '**1**' for deny action (count from bit0 to bit31 and right to left)

Changes in CLI

The following CLI changes are included in Hyperscale firewall for FortiOS 7.2.4 Build 1396. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
771857	Firewall virtual IP (VIP) features that are not supported by hyperscale firewall policies are no longer visible from the CLI or GUI when configuring firewall VIPs in a hyperscale firewall VDOM. The following options are no longer available for IPv4 firewall VIPs (configured with the `config firewall vip` command) in hyperscale firewall VDOM: • `src-filter` • `service` • `nat44` • `nat46` • `arp-reply` • `nat-source-vip` • `portforward` • `srcintf-filter` The following options are no longer available 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` • `nat64`

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 7.2.4 Build 1396. The Special notices described in the FortiOS 7.2.4 release notes also apply to Hyperscale firewall for FortiOS 7.2.4 Build 1396.

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 7.2.4, 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 7.2.4 incompatibilities and limitations

Hyperscale firewall for FortiOS 7.2.4 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 Policy-based NGFW Mode.
- 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.
- Access control list (ACL) policies added to a hyperscale firewall VDOM that is processing traffic may take longer than expected to become effective. During a transition period, traffic that should be blocked by the new ACL policy will be allowed.
- 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.

- If hardware logging is configured to send log messages directly from NP7 processors (`log-processor` is set to `hardware`) (also called log2hw) and the log server group is configured to send log messages at the start and end of each session (`log-mode` is set to `per-session`), hardware logging may send multiple session start log messages, each with a different start time. Creating multiple session start log messages is a limitation of NP7 processor hardware logging, caused by the NP7 processor creating extra session start messages if session updates occur. You can work around this issue by:
  - Setting `log-mode` to `per-session-ending`. This setting creates a single log message when the session ends. This log message records the time the session ended as well as the duration of the session. This information can be used to calculate the session start time.
  - Setting `log-processor` to `host` (also called log2host). Host hardware logging removes duplicate log start messages created by the NP7 processor. Host logging may reduce performance.
- 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 7.2.4 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 firmware and is licensed for hyperscale firewall features, you can follow a normal firmware upgrade process to upgrade to FortiOS 7.2.4.

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 7.2.4. Once you have upgraded to 7.2.4 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 7.2.4. After upgrading, you should review all NAT64 and NAT46 firewall policies and all VIP64 and VIP46 firewall policies added prior to upgrading.

In FortiOS 7.2.4, you apply hyperscale firewall features by creating normal firewall policies in hyperscale firewall VDOMs. FortiOS 7.2.4 no longer has hyperscale firewall policies in a separate hyperscale firewall policy list, as supported by FortiOS 6.2 and 6.4.

The FortiOS 7.2.4 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 11.

Product integration and support

The Product integration and support information described in the FortiOS 7.2.4 release notes also applies to Hyperscale firewall for FortiOS 7.2.4 Build 1396.

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 7.2.4 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 7.2.4 Build 1396. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 7.2.4 release notes also apply to Hyperscale firewall for FortiOS 7.2.4 Build 1396.

Bug ID	Description
724085	NP7 processors no longer support offloading sessions that will pass through two EMAC-VLAN interfaces. This includes traffic passing through an EMAC-VLAN interface when the parent interface is in another VDOM. This means that traffic will no longer be blocked when it passes through two EMAC-VLAN interfaces with offloading enabled. Instead, the traffic will be processed by the CPU and will not be offloaded to NP7 processors.

775793	You can use the following command to record traffic shaper statistics for sessions offloaded to NP7 processors:
	`config system npu`
	`  set shaping-stats {disable | enable}`
	`end`
	With this option enabled, FortiOS records traffic shaping statistics for sessions offloaded to NP7 processors in the same way as sessions that are processed by the CPU.
	To record traffic shaping statistics for offloaded NP7 sessions, the NP7 processors must be operating in policing traffic shaping mode.

777924	You can use the following command to protect a FortiGate with NP7 processors from non-SYN TCP attacks:
	`configure system npu`
	`  set ple-non-syn-tcp-action {drop | forward}`
	`end`
	By default this option is set to `forward`, and the NP7 policy lookup engine (PLE) sends TCP local-in non-SYN packets that are from TCP sessions that haven't been established to the CPU. If your FortiGate performance is affected by large numbers of local-in non-SYN packets, you can set this option to `drop`, causing the NP7 PLE to drop TCP local-in non-SYN packets.

780315	Resolved an issue that reduces connections per second (CPS) performance for VLAN traffic.
804742 810366	Resolved a memory-related issue that caused it to take longer than expected for hyperscale firewall policy changes to be applied to traffic. The delay affected offloaded NP7 traffic and CPU traffic
805179	Resolved an issue that blocked traffic that could be offloaded to NP7 processors when that traffic passes through a VXLAN interface that is part of a software switch.
807476	Packet buffers are now successfully cleaned up after going through host interface TX/RX queues.
809030	Resolved an issue that could sometimes cause traffic accepted by hyperscale firewall policies with port block allocation (PBA) IP pools to be dropped. The problem could occur after changing the hyperscale firewall policy configuration.
809623	Resolved an issue that caused CAPWAP traffic to be dropped when CAPWAP offloading is enabled for FortiGates with NP7 processors.

Bug ID	Description
813314	Resolved an issue with how the GUI and CLI displays information about single port allocation CGN IP pools.
815253 825523	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.
815360	Resolved an issue that could cause FortiGates with NP7 processors to encounter a kernel panic when deleting more than two hardware switches at the same time.
816385	Resolved an issue that could cause FortiGates with NP7 processors to display a message similar to `rcu_sched self-detected stall on CPU` on console and freeze. This would occur after enabling NP7 `capwap-offload` or sending inner VLAN traffic and restarting FortiOS or upgrading the firmware.
819872	Resolved an issue affecting FortiGates with NP7 processors in an FGCP HA cluster that could cause a kernel panic and lost heartbeat packets. The issue could also result in an HA split brain scenario after a firmware upgrade.
821320	Resolved an issue that caused NP7 processors to drop L2 tunneled VLAN wireless client traffic when CAPWAP offloading is enabled.
824733	Resolved a routing synchronization issue that sometimes caused IPv6 static routes to continue to be active in VDOMs after they have been deleted from the configuration.
826719	Resolved an issue that caused incorrect hardware session counts to be displayed on the GUI or CLI after deleting multicast sessions.
831672 835697 836443	Interface routes are now successfully deleted from the NP7 LPM routing table after moving an interface to a different VDOM. This change also resolves an issue with DHCP servers on interfaces in hyperscale firewall VDOMs
834762 836049	Resolved an issue that could cause a kernel panic on FortiGates with NP7 processors in an FGCP HA cluster.
836474	Changing the zone configuration of a hyperscale firewall VDOM is now supported by the hyperscale firewall policy engine.
836687 837682	Improved the accuracy of statistics collected from hardware logging.
837270 857311	Allowing intra-zone traffic is now supported in hyperscale firewall VDOMs. Options to block or allow intra-zone traffic are available on the GUI and CLI.
843305	A message similar to PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS no longer appears on the console error log when a FortiGate with NP7 processors starts up.
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 received an HASYNC message from the secondary FortiGate.
856264 859171	Resolved an issue with how NP7 processors process large packets or fragmented packets in hairpin traffic.
861442	Unsupported ZTNA options removed from hyperscale firewall policies.

Bug ID	Description
863520	Resolved an issue that could cause incorrect session counts for NP7 sessions passing through non-hyperscale VDOMs of a FortiGate with hyperscale features enabled.
864495	Resolved an issue that caused the GUI to display incorrect resource statistics for CGN resource allocation IP pool groups.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 7.2.4 Build 1396. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 7.2.4 release notes also apply to Hyperscale firewall for FortiOS 7.2.4 Build 1396.

Bug ID	Description
802182	If you have configured a hardware logging server to use a VLAN interface to send log messages to a remote log server, you can't change the VLAN ID of the VLAN interface. Instead an error message similar to the following appears on the CLI when you attempt to change the VLAN ID: `cmdb_txn_cache_data (query=log.npu-server,leve=1) failed`. You can work around this issue by removing the hardware logging server or changing its destination, changing the VLAN ID of the VLAN interface, and then restoring the configuration of the hardware logging server.
807523	On NP7 platforms, the `config system npu` option `nat46-force-ipv4-packet-forwarding` is missing.
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.
841712	The `config system npu` option `nat64-force-ipv4-packet-forwarding` is not available.
843197	The output of the `diagnose sys npu-session list/list-full` command does not include policy route information.
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.
872146	In a hyperscale firewall VDOM, intra-zone policy sessions are assigned incorrect policy IDs.

www.fortinet.com