Hyperscale Firewall - Release Notes

Version 6.2.6 Build 6988

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 11, 2023
Hyperscale Firewall 6.2.6 Build 6988 Release Notes
01-626-688354-20230111

TABLE OF CONTENTS

Change log 4

Hyperscale firewall for FortiOS 6.2.6 release notes 5

Supported FortiGate models 5

What's new 6

Hyperscale firewall features enabled per VDOM 6

Hyperscale firewall VDOMs require a specific naming convention 6

Enabling hyperscale firewall features per VDOM 7

Hyperscale firewall GUI changes 8

Hyperscale firewall policies 8

Hyperscale firewall policy options 8

CGNAT features in IPv4 and NAT64 firewall policies 9

Hardware logging in a firewall policy 9

Hyperscale hardware logging servers 10

Hyperscale firewall CLI changes 10

Enable hyperscale firewall features 10

Special hyperscale firewall VDOM naming convention 10

Hyperscale firewall policy 11

Hyperscale firewall inter-VDOM link acceleration 12

Host hardware logging 12

Hardware logging NetFlow template packet timeout 12

Hyperscale firewall SNMP MIB and trap fields 13

IP pool MIB and trap fields 13

Hyperscale firewall policy MIB fields 13

Hyperscale firewall inter-VDOM link acceleration 14

NP7 hyperscale firewall packet sniffer 15

Packet sniffer examples 16

Special notices 17

Hyperscale firewall 6.2.6 incompatibilities and limitations 17

About hairpinning 18

Interface device identification is not compatible with hyperscale firewall traffic 18

Upgrade information 19

To upgrade an HA cluster 19

To upgrade a standalone FortiGate 20

Product integration and support 21

Maximum values 21

Resolved issues 22

Known issues 23

Change log

Date	Change description
January 11, 2023	Added more information about `arp-reply` support limitations for IPv4 and IPv6 firewall VIPs to Hyperscale firewall 6.2.6 incompatibilities and limitations on page 17.
November 22, 2022	Corrections to Hyperscale firewall VDOMs require a specific naming convention on page 6.
October 18, 2021	Removed the incorrect statement "NP7 fragment reassembly is not supported" from Hyperscale firewall 6.2.6 incompatibilities and limitations on page 17. See Reassembling fragmented packets for information about supporting NP7 fragment reassembly.
June 7, 2021	New section: Interface device identification is not compatible with hyperscale firewall traffic on page 18.
March 24, 2021	Added information about hyperscale firewall VDOMs not supporting profile-based NGFW firewall policies and consolidated firewall policies to Hyperscale firewall 6.2.6 incompatibilities and limitations on page 17. Added known issue 704140 to Known issues on page 23.
March 19, 2021	Removed a reference to sessions generated with a Syn type not being supported from Hyperscale firewall 6.2.6 incompatibilities and limitations on page 17.
March 18, 2021	Added known issue 703667 to Known issues on page 23. Added information about hyperscale firewall VDOMs not supporting central NAT to Hyperscale firewall 6.2.6 incompatibilities and limitations on page 17.
March 8, 2021	Removed known issue 700271 because this issue only applies to FortiGates with NP7 processors that are not licensed for hyperscale firewall features. This known issue will be added the FortiOS 6.2.6 release notes.
March 5, 2021	Added known issue 700271 to Known issues on page 23.
March 1, 2021	Added known issue 695455 to Known issues on page 23.
February 22, 2021	Updates to NP7 hyperscale firewall packet sniffer on page 15.
February 19, 2021	Improvements and corrections to What’s new on page 6.
February 17, 2021	New section: Hyperscale firewall SNMP MIB and trap fields on page 13. Fixed some errors and broken links.
February 12, 2021	Initial version.

Hyperscale firewall for FortiOS 6.2.6 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 6.2.6 Build 6988.

In addition, special notices, new features and enhancements, changes in CLI defaults, changes in default values, changes in table size, product integration and support, resolved issues, known issues, and limitations described in the FortiOS 6.2.6 Release Notes also apply to FortGates licensed for Hyperscale firewall features for FortiOS 6.2.6 Build 6988.

For Hyperscale firewall documentation for this release, see the Hyperscale Firewall Guide.

Supported FortiGate models

Hyperscale firewall for FortiOS 6.2.6 Build 6988 supports the following models. The information in these release notes applies to these FortiGate models if they are licensed for Hyperscale firewall features.

- FortiGate-1800F
- FortiGate-1801F
- FortiGate-2600F
- FortiGate-2601F
- FortiGate-4200F
- FortiGate-4201F
- FortiGate-4400F
- FortiGate-4401F

What’s new

The following new features have been added to Hyperscale firewall for FortiOS 6.2.6 Build 6988. The changes in the CLI, changes in GUI behavior, changes in default behavior, changes in table size, and new features or enhancements are described in the FortiOS 6.2.6 release notes also apply to Hyperscale firewall for FortiOS 6.2.6 Build 6988.

Hyperscale firewall features enabled per VDOM

Hyperscale firewall features are enabled per VDOM. To apply hyperscale firewall features, your FortiGate must be operating in multi VDOM mode. You cannot use the root VDOM for hyperscale firewall features. Instead you must create new hyperscale firewall VDOMs for the traffic that you want to apply hyperscale firewall features to.

You can also use the root VDOM for other traffic or create other VDOMs for other traffic.

Hyperscale firewall VDOMs require a specific naming convention

New for FortiOS 6.2.6, VDOMs in which you will be enabling hyperscale firewall features must be created with a special VDOM name that also includes a VDOM ID. The VDOM ID is used by FortiOS to create a kernel VDOM_ID for the VDOM that NP7 processors use to track hyperscale firewall sessions for that VDOM.

The number of hyperscale firewall VDOMs that you can create, depends on your hyperscale firewall license and is controlled by the following configuration option

```
config system global
   set hyper-scale-vdom-num <vdom-id-num>
end
```

By default `<vdom-id-num>` is set to the maximum number of hyperscale VDOMs that the FortiGate is licensed for. You can manually change the `<vdom-id-num>` if you want to limit the number of hyperscale VDOMs that can be created. The `<vdom-id-num>` range is 1 to 250.

Use the following syntax to create a hyperscale firewall VDOM:

```
config vdom
   edit <name>-hw<vdom-id>
end
```

Where:

`<name>` is a string that can contain any alphanumeric upper or lower case characters and the - and _ characters. The name cannot contain spaces and you should not use `-hw` in the name.

`<vdom-id>` a VDOM ID number in the range from 1 to `<vdom-id-num>`. For example, if your FortiGate is licensed for 250 hyperscale firewall VDOMs, if you haven't used the `hyper-scale-vdom-num` option to change the number of hyperscale firewall VDOMs, <vdom-id> can be from 1 to 250. Each hyperscale firewall VDOM must have a different <vdom-id>.

When you add a new hyperscale firewall VDOM with a <vdom-id>, FortiOS calculates the kernel VDOM_ID using the following formula:

```
kernel VDOM_ID = 501 - <vdom-id>
```

If you include leading zeros in the <vdom-id>, the kernel removes them when creating the ID. So avoid using leading zeros in the <vdom-id> to keep from accidentally creating duplicate IDs.

The VDOM name, including the <string>, -hw, and <vdom-id> can include up to 11 characters. For example, the VDOM name GCN-1-hw23 is valid but GCN-1234-hw23 is too long.

When you create a new hyperscale firewall VDOM, the CLI displays an output line that includes the VDOM name followed by the kernel VDOM_ID. For example:

```
config vdom
   edit Test01-hw150
   current vf=Test01-hw150:351
```

In this example, the kernel VDOM_ID is 351.

Another example:

```
config vdom
   edit Test02-hw2
   current vf=Test02-hw2:499
```

In this example, the kernel VDOM_ID is 499.

When you create a VDOM from the CLI, the new hyperscale VDOM becomes the current VDOM. The new hyperscale firewall VDOM may not appear in the VDOM list on the GUI until you log out of the GUI and then log back in.

Enabling hyperscale firewall features per VDOM

Use the following global command to enable hyperscale firewall features for your FortiGate:

```
config system npu
   set policy-offload-level full-offload
end
```

Once you have enabled global hyperscale firewall features, you must edit each hyperscale firewall VDOM and use the following command to enable hyperscale firewall features for that VDOM.

```
config system settings
   set policy-offload-level full-offload
end
```

The following options are also available for this command:

default set this VDOM to use the global policy-offload-level setting.

dos-offload enable offloading sessions to the NP7 processors, but without enabling hyperscale firewall features.

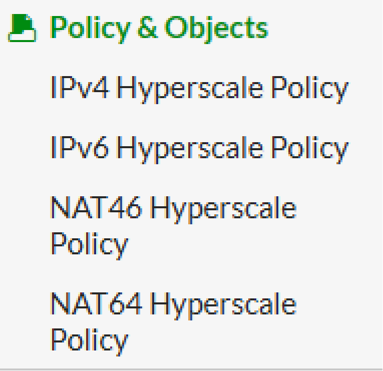
full-offload enable hyperscale firewall features for the current hyperscale firewall VDOM.

Hyperscale firewall GUI changes

When hyperscale firewall features are enabled for your Hyperscale firewall for FortiOS 6.2.6 Build 6988, the GUI has the following changes:

Hyperscale firewall policies

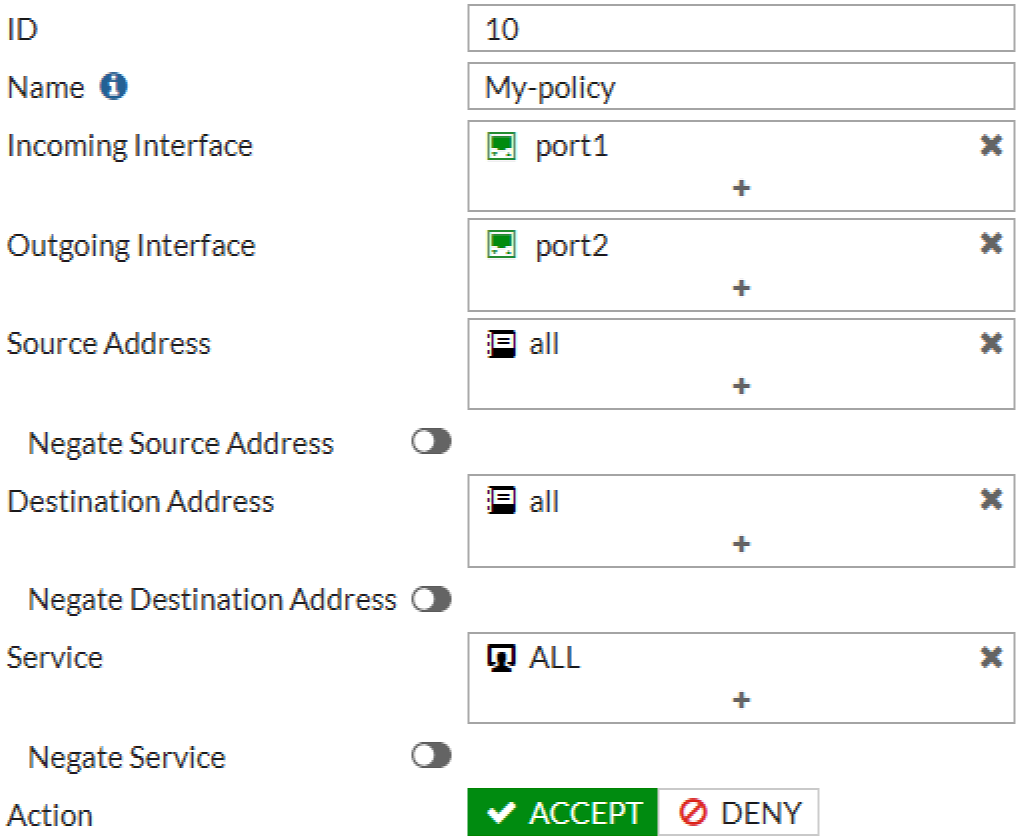
Only hyperscale firewall policies are available.



If you are upgrading your hyperscale firewall configuration from FortiOS 6.2.5 to 6.2.6 you must re-configure all of your hyperscale firewall policies using the new 6.2.6 hyperscale firewall policies.

Hyperscale firewall policy options

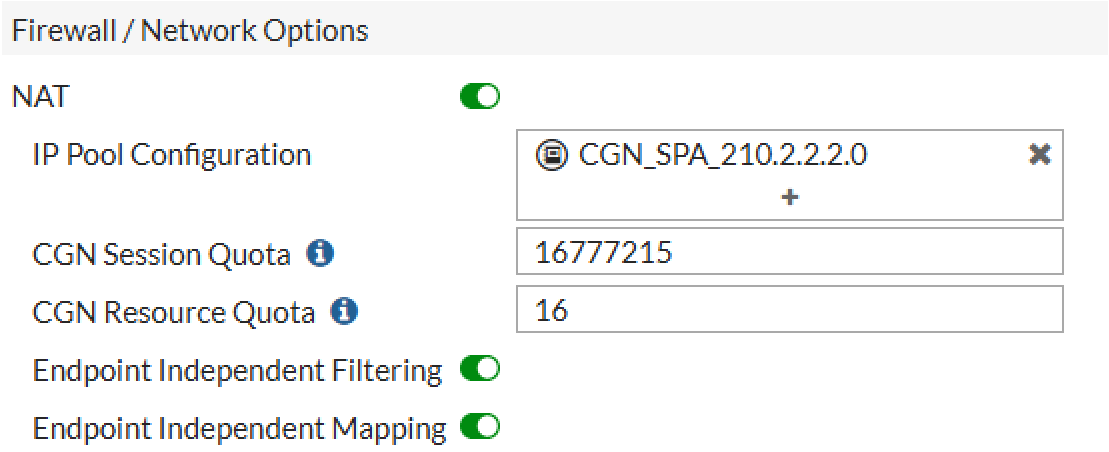
Hyperscale firewall policies have similar options to normal firewall policies for selecting traffic for which to offload session setup. Hyperscale firewall policies do not support UTM or NGFW features.



ID	10
Name	My-policy
Incoming Interface	port1
Outgoing Interface	port2
Source Address	all
Negate Source Address	○
Destination Address	all
Negate Destination Address	○
Service	ALL
Negate Service	○
Action	✓ ACCEPT / DENY

CGNAT features in IPv4 and NAT64 firewall policies

IPv4 and NAT64 Hyperscale firewall policies allow you to configure carrier grade NAT (CGNAT) options.

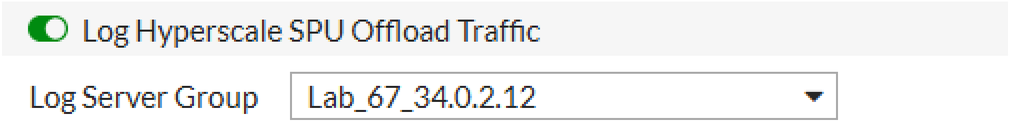


Firewall / Network Options

NAT	●
IP Pool Configuration	CGN_SPA_210.2.2.2.0
CGN Session Quota	16777215
CGN Resource Quota	16
Endpoint Independent Filtering	●
Endpoint Independent Mapping	●

Hardware logging in a firewall policy

You can also add hardware logging to a Hyperscale firewall policy.



Log Hyperscale SPU Offload Traffic

Log Server Group: Lab_67_34.0.2.12

Hyperscale hardware logging servers

You can set up multiple hyperscale hardware logging servers and add them to server groups. This is a global feature. If multiple VDOMs are enabled, all VDOMs can use these globally configured servers. To configure hardware logging, go to **Log & Report > Hyperscale SPU Offload Log Settings**.

Hyperscale firewall CLI changes

When hyperscale firewall features are enabled for your Hyperscale firewall for FortiOS 6.2.6 Build 6988, the CLI has the following changes:

Enable hyperscale firewall features

Use the following global command to enable hyperscale firewall features:

```
config system npu
   set policy-offload-level full-offload
end
```

Use the following command to enable hyperscale firewall features for the FortiGate or if multiple VDOMs are enabled, to enable or disable hyperscale firewall features for any VDOM:

```
config system settings
   set policy-offload-level full-offload
end
```

Special hyperscale firewall VDOM naming convention

VDOMs in which you will be enabling hyperscale firewall features must be created with a special VDOM name that also includes a VDOM ID number.

The following option can be used to set the VDOM ID range:

```
config system global
   set hyper-scale-vdom-num
end
```

By default this option is set to 250, allowing you to configure up to 250 hyperscale firewall VDOMs by setting the VDOM in the range of 1 to 250.

Use the following syntax to create a hyperscale firewall VDOM from the global CLI:

```
config vdom
```

```
   edit <string>-hw<vdom-id>
```

For information about how to name hyperscale firewall VDOMs, see Hyperscale firewall VDOMs require a specific naming convention on page 6.

Hyperscale firewall policy

The following hyperscale firewall policy commands are available in a hyperscale firewall VDOM:

```
config firewall hyperscale-policy
config firewall hyperscale-policy46
config firewall hyperscale-policy6
config firewall hyperscale-policy64
```

The `policy`, `policy6`, `policy46`, and `policy64` commands appear in the CLI but they cannot be configured.

If you are upgrading your hyperscale firewall configuration from FortiOS 6.2.5 to 6.2.6 you must re-configure all of your hyperscale firewall policies using the new 6.2.6 hyperscale firewall policies.

Here is the CLI syntax for the `config firewall hyperscale-policy` command:

```
config firewall hyperscale-policy
   edit 1
      set name <name>
      set scrcintf <interface>
      set dstintf <interface>
      set scraddr <address>
      set dstaddr <address>
      set action {accept | deny}
      set status {enable | disable|
      set service <service>
      set auto-asic-offload {enable | disable)
      set cgn-session-quota <quota>
      set cgn-resource-quota <quots>
      set cgn-eif {disable | enable}
      set cgn-eim {disable | enable}
      set cgn-log-server-grp <group-name>
      set tcp-timeout-pid <profile>
      set udp-timeout-pid <profile>
      set ippool {disable | enable}
      set poolname <cgn-ippool-name>
      set comments <comment>
      set srcaddr-negate {disable | enable}
      set dstaddr-negate {disable | enable
      set service-negate {disable | enable}
      set traffic-shaper <shaper>
      set traffic-shaper-reverse <shaper>
      set nat {disable | enable}
   end
```

Hyperscale firewall inter-VDOM link acceleration

You apply NP7 acceleration to inter-VDOM link traffic by creating inter-VDOM links with the `type` set to `npupair`. For example:

```
config system vdom-link
   edit <name>
      set type npupair
   end
```

Host hardware logging

Hyperscale firewall hardware logging for FortiOS 6.2.6 Build 6988 includes a new hardware logging mode host logging. Host logging uses the FortiGate CPU for hardware logging instead of NP7 processors.

Use the following command to configure host logging:

```
config log npu-server
   set log-processor host
end
```

If you set `log-processor` to `host`, all hardware logging functions are supported and the hardware logging configuration is the same with the following limitations:

- Setting `log-processor` to `host` can reduce overall FortiGate performance because the FortiGate CPUs handle hardware logging instead of offloading logging to the NP7 processors.
- Host logging may not provide the NHI, stats, OID, gateway, expiration, and duration information for short-lived sessions.
- Host logging does not support Netflow v9.

Hardware logging NetFlow template packet timeout

You can use the hardware logging option `template-tx-timeout` to configure how often the hyperscale firewall FortiGate sends NetFlow template updates to the log server. Use the following command to change the NetFlow template timeout:

```
config log npu-server
   config server-info
      edit <index>
         set template-tx-timeout <timeout>
      end
```

`template-tx-timeout` the time interval between sending NetFlow template packets. NetFlow template packets communicate the format of the NetFlow messages sent by the FortiGate to the NetFlow server. Since the message format can change if the NetFlow configuration changes, the FortiGate sends template updates at regular intervals to make sure the server can correctly interpret NetFlow messages. The timeout range is from 60 to 86,400 seconds. The default timeout is 600 seconds.

Hyperscale firewall SNMP MIB and trap fields

IP pool MIB and trap fields

You can use the following MIB fields to get hyperscale firewall IP pool information:

```
FgFwIppStatsEntry ::= SEQUENCE {
    ...
    fgFwIppStatsFlags         DisplayString,
    fgFwIppStatsGroupName     DisplayString,
    fgFwIppStatsBlockSize     Gauge32,
    fgFwIppStatsPortStart     InetPortNumber,
    fgFwIppStatsPortEnd       InetPortNumber,
    fgFwIppStatsStartClientIP IpAddress,
    fgFwIppStatsEndClientIP   IpAddress,
    fgFwIppStatsRscTCP        Gauge32,
    fgFwIppStatsRscUDP        Gauge32,
    fgFwIppStatsUsedRscTCP    Gauge32,
    fgFwIppStatsUsedRscUDP    Gauge32,
    fgFwIppStatsPercentageTCP Gauge32,
    fgFwIppStatsPercentageUDP Gauge32
}
```

The following SNMP trap is also available for IP pool utilization:

```
fgTrapPoolUsage NOTIFICATION-TYPE
    OBJECTS     { fnSysSerial, sysName, fgFwIppTrapType, fgFwIppStatsName,
fgFwIppStatsGroupName, fgFwTrapPoolUtilization, fgFwIppTrapPoolProto }
    STATUS      current
    DESCRIPTION
        "A trap for ippool."
    ::= { fgTrapPrefix 1401 }
```

Hyperscale firewall policy MIB fields

You can use the following MIB fields to send SNMP queries for hyperscale firewall policy information. These MIB fields support IPv4 and IPv6 hyperscale firewall policies and are available from the latest FORTINET-FORTIGATE-MIB.mib.

Path: FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgFirewall.fgFwPolicies.fgFwPolTables

OID: 1.3.6.1.4.1.12356.101.5.1.2

Index	MIB field	Description
.3	fgFwHsPolStatsTable	IPv4 hyperscale firewall policy statistics table.
.3.1	fgFwHsPolStatsEntry	IPv4 hyperscale firewall policy statistics entry.

Index	MIB field	Description
.3.1.1	fgFwHsPolID	IPv4 hyperscale firewall policy ID.
.3.1.2	fgFwHsPolPktCount	IPv4 hyperscale firewall policy packet count.
.3.1.3	fgFwHsPolByteCount	IPv4 hyperscale firewall policy byte count.
.3.1.4	fgFwHsPolLastUsed	The last date and time the Ipv4 hyperscale firewall policy was used to start a session.
.4	fgFwHsPol6StatsTable	IPv6 hyperscale firewall policy stats table.
.4.1	fgFwHsPol6StatsEntry	IPv6 hyperscale firewall policy statistics entry.
.4.1.1	fgFwHsPol6ID	IPv6 hyperscale firewall statisticsID.
.4.1.2	fgFwHsPol6PktCount	IPv6 hyperscale firewall policy packet count.
.4.1.3	fgFwHsPol6ByteCount	IPv6 hyperscale firewall policy byte count.
.4.1.4	fgFwHsPol6LastUsed	The last date and time the IPv6 hyperscale firewall policy was used to start a session.

Queries of these fields follow the convention `.oid.<vdom-id>.<policy-id>`

Example SNMP query for IPv4 hyperscale firewall policy statistics:

```
$ snmpwalk -v2c -c public <ip-address> 1.3.6.1.4.1.12356.101.5.1.2.3.1
```

Example SNMP query for IPv6 hyperscale firewall policy statistics:

```
$ snmpwalk -v2c -c public <ip-address> 1.3.6.1.4.1.12356.101.5.1.2.4.1
```

Hyperscale firewall inter-VDOM link acceleration

If hyperscale firewall support is enabled, you apply NP7 acceleration to inter-VDOM link traffic by creating inter-VDOM links with the `type` set to `npupair`. For example:

```
config system vdom-link
   edit <name>
      set type npupair
   end
```

The command creates a pair of interfaces that are connected logically. For example, the following command:

```
config system vdom-link
   edit vdom-link0
      set type npupair
   end
```

Creates two interfaces, named `vdom-link00` and `vdom-link01`.

The default NPU VDOM inter-VDOM links (for example npu0_vlink0, npu0_vlink1, npu1_vlink0, and so on) are not supported for links to or from VDOMs with hyperscale firewall acceleration enabled.

NP7 hyperscale firewall packet sniffer

You can use the following command as a hyperscale firewall packet sniffer. This packet sniffer displays information about packets offloaded by NP7 processors. You can also use this command to mirror sniffed packets to a FortiGate interface.

```
diagnose npu sniffer {start | stop | filter}
```

Use `start` and `stop` to start or stop displaying packets on the CLI. Before the sniffer will start you need to use the `filter` to specify the packets to display. Use the command `diagnose sniffer packet npudbg` to display sniffed packets on the CLI.

Use `filter` to create a definition of the types of packets to display. Filter options include:

`selector` you can create up to four filters (numbered 0 to 3). Use this command to create a new filter or select the stored filter to be used when you start the packet sniffer. You can also use this command to have multiple filters active at one time. See below for an example of sniffing using multiple active filters.

`intf <interface-name>` the name of an interface to display packets passing through that interface.

`dir {0 | 1 | 2}` the direction of the packets passing through the interface. `0` displays ingress packets, `1` displays egress packets, and `2` displays both ingress and egress packets.

`ethtype <type>` the ethertype of the packets to sniff if you want to see non-IP packets.

`protocol <number>` the IP protocol number of the packets to sniff in the range 0 to 255. The packet sniffer can only sniff protocols that can be offloaded by the NP7 processors.

`srcip <ipv4-ip-address>/<ipv4-mask>` an IPv4 IP address and netmask that matches the source address of the packets to be sniffed.

`dstip <ipv4-ip-address>/<ipv4-mask>` an IPv4 IP address and netmask that matches the destination address of the packets to be sniffed.

`ip <ipv4-ip-address>/<ipv4-mask>` an IPv4 IP address and netmask that matches a source or destination address in the packets to be sniffed.

`srcip6 <ipv6-ip-address>/<ipv6-mask>` an IPv6 IP address and netmask that matches the source address of the packets to be sniffed.

`dstip6 <ipv6-ip-address>/<ipv6-mask>` an IPv6 IP address and netmask that matches the destination address of the packets to be sniffed.

`ip6 <ipv6-ip-address>/<ipv6-mask>` an IPv6 IP address and netmask that can match source or destination addresses in the packets to be sniffed.

`sport <port-number>` layer 4 source port of the packets to be sniffed.

`dport <port-number>` layer 4 destination port of the packets to be sniffed.

`port <port-number>` layer 4 source or destination port of the packets to be sniffed.

`outgoing_intf <interface>` the name of the interface out of which to send mirrored traffic matched by the filter.

`outgoing_vlan <vlan-id>` the VLAN ID added to mirrored traffic matched by the filter and sent out the mirror interface.

`clear` clear all filters.

Packet sniffer examples

First, a basic example to sniff offloaded TCP packets received by the port23 interface. In the following example:

- The first line clears the filter.
- The second line sets the sniffer to look for packets on port23.
- The third line looks for packets exiting the interface.
- The fourth line looks for TCP packets.
- The fifth line starts the sniffer.
- The sixth line starts displaying the packets on the CLI.

```
diagnose npu sniffer filter
diagnose npu sniffer filter intf port23
diagnose npu sniffer filter dir 2
diagnose npu sniffer filter protocol 6
diagnose npu sniffer start

diagnose sniffer packet npudbg
```

Second, an example that uses the following two filters:

- The first filter, selector 0, looks for incoming and outgoing TCP packets on port1.
- The second filter, selector 1, looks for outgoing UDP packets on port2.
- The final line starts displaying packets for both filters on the CLI.

```
diagnose npu sniffer filter selector 0
diagnose npu sniffer filter intf port1
diagnose npu sniffer filter protocol 6
diagnose npu sniffer filter dir 2
diagnose npu sniffer start

diagnose npu sniffer filter selector 1
diagnose npu sniffer filter intf port2
diagnose npu sniffer filter protocol 17
diagnose npu sniffer filter dir 1
diagnose npu sniffer start

diagnose sniffer packet npudbg
```

Special notices

This section highlights some of the operational changes and other important features that administrators should be aware of for Hyperscale firewall for 6.2.6 Build 6988. The Special notices described in the FortiOS 6.2.6 release notes also apply to Hyperscale firewall for FortiOS 6.2.6 Build 6988.

Hyperscale firewall 6.2.6 incompatibilities and limitations

Hyperscale firewall for FortiOS 6.2.6 has the following limitations and incompatibilities with FortiOS features:

- Proxy or flow based inspection is not supported. You cannot include security profiles in hyperscale firewall policies.
- Single-sign-on authentication including FSSO and RSSO is not supported. Other types of authentication are supported.
- IPsec VPN is not supported. You cannot create hyperscale firewall policies where one of the interfaces is an IPsec VPN interface.
- Hyperscale firewall VDOMs do not support Central NAT.
- Hyperscale firewall VDOMs do not support profile-based NGFW firewall policies.
- Hyperscale firewall VDOMs do not support consolidated firewall policies.
- Hyperscale firewall VDOMs must be NAT mode VDOMs. Hyperscale firewall features are not supported for transparent mode VDOMs.
- Hyperscale firewall VDOMs do not support traffic shaping policies or profiles. Only outbandwidth traffic shaping is supported for hyperscale firewall VDOMs.
- Traffic shaping with queuing using the NP7 QTM module is not compatible with carrier-grade NAT and hyperscale firewall features. See NP7 traffic shaping.
- The proxy action is not supported for DoS policy anomalies in hyperscale firewall VDOMs.
- 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 6.2.6 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.

FortiOS 6.2.6 is the first Hyperscale firewall release for the FortiGate-1800F, 1801F, 2600F, and 2601F. To use hyperscale firewall features with these models, follow the upgrade path to upgrade the firmware to FortiOS 6.2.6, activate your hyperscale firewall license, and then configure hyperscale Firewall features.

If you are currently operating a FortiGate-4200F, 4201F, 4400F, or 4401F with a hyperscale firewall license, upgrading to FortiOS 6.2.6 will remove the existing hyperscale firewall configuration but the hyperscale firewall license will still be active. You can go ahead and create a new hyperscale firewall configuration for FortiOS 6.2.6.

If you are currently operating a FortiGate-4200F, 4201F, 4400F, or 4401F without a hyperscale firewall license you can use the upgrade path to upgrade to FortiOS 6.2.6. To configure hyperscale firewall features, activate your hyperscale firewall license and set up the hyperscale firewall configuration.

⚠ The FortiOS 6.2.6 hyperscale firewall configuration is very different from the 6.2.5 configuration. Upgrading a FortiGate-4200F, 4201F, 4400F, or 4401F from FortiOS 6.2.5 to 6.2.6 will require significant time for preparation and planning before the firmware upgrade and significant downtime after the firmware upgrade to create the new configuration.

To upgrade an HA cluster

Recommended procedure for upgrading an HA cluster,

1. Disconnect the backup FortiGate from the cluster.
2. Upgrade the backup FortiGate's firmware to FortiOS 6.2.6 and set the configuration to factory defaults.
3. Create the new FortiOS 6.2.6 hyperscale firewall configuration on the backup FortiGate.

   Fortinet Support can assist with setting up the new configuration.
4. When the backup FortiGate is reconfigured and the configuration tested you can swap network connections from the primary FortiGate to the backup FortiGate with minimal downtime.
5. Then you can upgrade the firmware on the primary FortiGate and reset it to factory defaults.
6. Apply the new hyperscale configuration to the primary FortiGate.

   Do this before reforming the cluster, since some configurations may require restarting the FortiGate.
7. Add the primary FortiGate back to the cluster to re-form the cluster.

To upgrade a standalone FortiGate

To upgrade a standalone FortiGate, Fortinet recommends preparing the new configuration on a test device if possible before configuring your production FortiGate. Fortinet Support can help with planning, configuration, and conversion.

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.

Product integration and support

This section describes Hyperscale firewall for FortiOS 6.2.6 Build 6988 product integration and support information. The Product integration and support information described in the FortiOS 6.2.6 release notes also applies to Hyperscale firewall for FortiOS 6.2.6 Build 6988.

Hyperscale firewall for FortiOS 6.2.6 Build 6988 requires the following or newer versions of FortiManager and FortiAnalyzer:

- FortiManager 6.2.7 (FortiManager 6.2.7 Release Notes) or 6.4.4 (FortiManager 6.4.4 Release Notes)
- FortiAnalyzer 6.2.7 (FortiAnalyzer 6.2.7 Release Notes) or 6.4.4 (FortiAnalyzer 6.4.4 Release Notes)

Maximum values

Maximum values for hyperscale firewall FortiGate models for FortiOS 6.2.6 are available from the FortiOS Maximum Values Table (https://docs.fortinet.com/max-value-table).

Resolved issues

The following issues have been fixed in Hyperscale firewall for FortiOS 6.2.6 Build 6988. For inquires about a particular bug, please contact Customer Service & Support. The Resolved issues described in the FortiOS 6.2.6 release notes also apply to Hyperscale firewall for FortiOS 6.2.6 Build 6988.

Bug ID	Description
670140	Resolved an issue with the NPD/LPM Route update sequence, which prevented some TCP sessions from being offloaded to NP7 processors.
670756	Resolved an issue that prevented offloading sessions in transparent mode VDOMs.
671170	Closed a PBA memory leak.
674167	Resolved an issue that caused a system crash when creating an inter-VDOM link.
676674	Resolved an issue that caused EoIP packets to be dropped by NP7processors if FP anomaly checking has the `ipv4-proto-err` option is set to `drop`.
677749	Created a VDOM naming workaround to make sure that VDOM IDs are the same on the primary and backup FortiGates in an FGCP HA cluster.
677751	Resolved a segmentation fault associated with policy routing for some kinds of traffic.
677825	Resolved an issue that caused VLANs to get incorrect virtual MAC addresses when switching to HA mode.
689269	Resolved an issue that prevented HA failover from working until the backup FortiGate is restarted.
689619	Resolved an issue that caused NP7 IPsec hardware acceleration to drop packets when the packets are larger than PMTU and smaller than the tunnel MTU.
689625	Resolved an issue with supporting some SFP transceivers on HA interfaces.
689735	Resolved an issue with HA hardware session synchronization that blocked sending session sync packets to traffic interfaces.

Known issues

The following issues have been identified in Hyperscale firewall for FortiOS 6.2.6 Build 6988. For inquires about a particular bug, please contact Customer Service & Support. The Known issues described in the FortiOS 6.2.6 release notes also apply to Hyperscale firewall for FortiOS 6.2.6 Build 6988.

Bug ID	Description

632955	Traffic shaping using traffic shaping policies is not supported. Other methods of traffic shaping are supported if the following configuration is used:
	`config system npu`
	`   set default-qos-type policing`
	`end`

633347	ECMP weight-based load balancing is not supported. Weight-based load balancing does not direct more traffic to routes with higher weights.
633401	HA hardware session synchronization is currently only supported between two FortiGates using a direct connection between the HA hardware session synchronization interfaces. You can't use a switch for this connection and you can't synchronize sessions between more than two FortiGates.
671590	FGSP failover may not work as expected.
675680	UDPv6 session are no longer offloaded to NP7 processors after deleting and then re-adding a hyperscale firewall policy for them.
676525	Sessions are lost if a policy route is deleted or an interface is shut down.
677749	For FortiOS 6.2.6, Hyperscale firewall VDOM names should be created using special naming conventions. See Hyperscale firewall VDOMs require a specific naming convention on page 6.
0678390	The `get system ha status` command should display information about the total number of hardware session-sync sessions.
684616	Per-session log messages for ICMP traffic accepted by a hyperscale firewall policy are not available.
684778	Hairpin configurations will only work if the firewall destination address is set to All.
0688221	The FortiGate MIB does not support traps or queries for NAT64 and NAT46 hyperscale firewall policies.
686971	Some TFTP functionality is not compatible with hyperscale firewall features.
683171	When viewing a hyperscale firewall policy from the GUI, the displayed Hit count is always 1.
692021	Only one hardware session synch interface can be configured in an HA configuration.
693159	If you have set up hardware logging to use the CPU to send log messages to a syslog server, after adding a new hyperscale firewall policy, there may be a delay of a few minutes before the FortiGate can correctly display information about traffic accepted by this policy. This includes traffic information displayed on the GUI or by using diagnose commands such as `diagnose sys npu-session list`. After this initial delay, the FortiGate will display current session information.

Bug ID	Description

	Example hardware logging configuration that can result in this issue:
	`config log npu-server`
	`   set log-processor host`
	`   ...`
	`      config server-group`
	`         edit <name>`
	`            set log-format syslog`
	`         end`

693930	If hardware logging using NetFlow is enabled, each NP7 processor sends a NetFlow template update message to configured NetFlow servers when the `template-tx-timeout` timer expires. If your FortiGate has multiple NP7 processors, the FortiGate will send multiple template update messages, one for each NP7 processor.
695275	It is possible to create a hyperscale firewall policy where the address range of an IP pool in the policy overlaps with the IP address of one or more destination servers. Traffic will not flow in this configuration because the system will not send ARP requests to the server. Future versions will prevent incorrectly configuring this kind of overlap.
695262	In a hyperscale firewall policy, setting the service to All and selecting Negate service causes a system error because this configuration is invalid.
695455	Under high CGNAT traffic load that causes high CPU usage and causes the FortiGate to enter conserve mode, the FortiGate may unexpectedly restart after writing an event log message similar to the following: `date=xxxxxxxx time=xxxxx logid="0100032200" type="event" subtype="system" level="critical" vd="root" eventtime=xxxxxxxxxxxxx tz="+0300" logdesc="Device shutdown" msg="Fortigate had experienced an unexpected power off!"` The problem is not related to the power system; the message appears and the restart occurs even though the power system is working correctly.
695527	Using the `diagnose sys npu-session list {46 | 64}` command to display NAT64 or NAT46 sessions being processed by the NP7 processor doesn't display any information if filtering options are enabled (for example, using the `diagnose sys npu-session filter ...` command).

695732	When setting up an FGCP cluster of two FortiGates with hyperscale firewall features enabled, both FortiGates to be added to the cluster must have the same split interface configuration. If the split interface configuration is different on one of the FortiGates, when it joins the cluster it will continuously restart. This occurs because splitting interfaces requires the FortiGate to restart and this mechanism currently does not work correctly when forming a cluster.
	The recommended workaround is to split the interfaces on both FortiGates before configuring HA. For example, use the following command to split port24:
	`config system global`
	`   set split-port "port24"`
	`end`
	Changing the split interface configuration is not recommended after the cluster has formed. If you need to change the split interface configuration, remove the FortiGates from the cluster and change the split interface configuration of each FortiGate separately and then set up the cluster again.

Bug ID	Description

695732	When setting up an FGCP cluster of two FortiGate-4200Fs, 4201Fs, 4400Fs, or 4401Fs with hyperscale firewall features enabled, both FortiGates to be added to the cluster must have the same `port-path-option` configuration:
	`config system npu`
	`   config port-path-option`
	`      set ports-using-npu {ha1 ha2 aux1 aux2}`
	`   end`
	If the `port-path-option` configuration is different on one of the FortiGates, when it joins the cluster it will continuously restart. This occurs because changing the `port-path-option` configuration requires the FortiGate to restart and this mechanism currently does not work correctly when forming a cluster.
	Changing the `port-path-option` configuration is not recommended after the cluster has formed. If you need to change the `port-path-option` configuration, remove the FortiGates from the cluster and change the `port-path-option` configuration of each FortiGate separately and then set up the cluster again.

696133	If your FortiGate has one hyperscale VDOM, IPv4 traffic matched by policy routes in that VDOM is offloaded by the NP7 processor as long as you edit the policy route twice. If you don't edit the policy route twice, the traffic is sent to the CPU. IPv6 traffic matched by IPv6 policy routes is always sent to the CPU. If your FortiGate has multiple hyperscale firewall VDOMs, for all VDOMs other than the first VDOM, IPv4 traffic matched by IPv4 policy routes is offloaded by the NP7 processor as long as you edit the policy route twice. If you don't edit the policy route twice, the traffic is dropped. IPv6 traffic matched by IPv6 policy routes is always dropped. It is recommended that you contact Fortinet Support for assistance with IPv4 or IPv6 policy routing in hyperscale firewall VDOMs
703667	FGCP HA hardware session synchronization may not synchronize all hyperscale firewall sessions to the backup FortiGate if the hyperscale firewall session includes one or more overload IP pools. The session loss rate on the backup FortiGate depends on the percentage of resource retries during session setup. The more IP pool resources that are available, the lower the session loss rate.
704140	The Sessions dashboard widget may incorrectly display a negative value for SPU sessions percentage.