FORTINET

Release Notes

FortiOS 8.0.0

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

FORTINET VIDEO LIBRARY
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 LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 21, 2026
FortiOS 8.0.0 Release Notes
01-800-1177322-20260421

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-04-21	Initial release of 8.0.0.

Introduction and supported models

This guide provides release information for FortiOS 8.0.0 build 0167.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 8.0.0 supports the following models.

FortiGate	FG-30G, FG-31G, FG-40F, FG-40F-3G4G, FG-50G, FG-51G, FG-50G-5G, FG-51G-5G, FG-50G-SFP, FG-50G-DSL, FG-50G-SFP-POE, FG-51G-SFP-POE, FG-60F, FG-61F, FG-70F, FG-71F, FG-70G, FG-71G, FG-70G-POE, FG-71G-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81F, FG-81F-POE, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-200E, FG-200F, FG-200G, FG-201E, FG-201F, FG-201G, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-700G, FG-701G, FG-800D, FG-900D, FG-900G, FG-901G, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000F, FG-3001F, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-30G, FWF-31G, FWF-40F, FWF-40F-3G4G, FWF-50G, FWF-50G-5G, FWF-50G-SFP, FWF-50G-DSL, FWF-51G, FWF-60F, FWF-61F, FWF-70G, FWF-71G, FWF-70G-POE, FWF-80F-2R, FWF-80F-2R-3G4G-DSL, FWF-81F-2R, FWF-81F-2R-3G4G-DSL, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-50G-5G, FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G, FGR-70G, FGR-70G-5G-Dual
FortiFirewall	FFW-1801F, FFW-2600F, FFW-3001F, FFW-3501F, FFW-3980E, FFW-4200F, FFW-4400F, FFW-4401F, FFW-4801F, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 8.0.0 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6001F, FG-6300F, FG-6301F, FG-6500F, FG-6501F
FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

FortiManager support for updated FortiOS private data encryption key

With the introduction of FortiOS 7.6.1, Fortinet has updated the private-data-encryption key feature. Administrators are no longer required to manually input a 32-digit hexadecimal `private-data-encryption` key. Instead administrators simply enable the command, and a random `private-data-encryption` key is generated.

How FortiManager 8.0.0 works with FortiOS private data encryption keys has changed. This topic covers the changes. See FortiManager behavior on page 10.

Previous FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
1234567890123456789012345678 9abc
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
1234567890123456789012345678 9abc
Your private data encryption key is accepted.
```

New FortiOS CLI behavior

```
config system global
    set private-data-encryption enable
end
This operation will generate a random private data encryption key!
Previous config files encrypted with the system default key cannot be restored after this
operation!
Do you want to continue? (y/n)y
Private data encryption key generation succeeded!
```

FortiManager behavior

FortiManager 8.0.0 can centrally manage FortiGates with the private-data-encryption setting enabled, with the following limitations:

- FortiManager can import objects that include the password type attribute.
  When FortiManager imports objects that include a password-type attribute, the administrator will be prompted to specify the password used by the object during the import process.
- FortiManager cannot be used to create NAT and transparent VDOMs.

This applies to FortiGates with private keys that are manually configured in FortiOS 7.6.0 and earlier and private keys that are randomly generated in FortiOS 7.6.1 and later.

FortiManager does not require you to verify the private key of the FortiGate when adding it to FortiManager.

FortiGates that require the protection of private data encryption and need to be managed by FortiManager should follow these procedures on a fresh install.

1. On the FortiGate, enable `private-data-encryption`.
2. On the FortiManager, add the FortiGate to the Device Manager. FortiManager will not be required to provide the key for PDE, as it will not be importing any password-related settings.
3. Make all configuration changes directly on the FortiManager.
4. Push and install the changes to the FortiGate.

If you require the use of NAT or Transparent VDOMs, you should perform this additional step before the steps above.

1. Enable `multi-vdom` mode on the FortiGate.
2. Add the VDOMs that you will use on the FortiGate.
3. Follow the above steps to enable `private-data-encryption` and manage the FortiGate from the FortiManager.

For more information, see the FortiManager Administration Guide.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 8.0.0 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 8.0.0 features.

- FortiGate 6000 incompatibilities and limitations
- FortiGate 7000E incompatibilities and limitations
- FortiGate 7000F incompatibilities and limitations

Agentless VPN (formerly SSL VPN web mode) not supported on some FortiGate series models

On the following FortiGate models, the Agentless VPN (formerly SSL VPN web mode) feature is no longer available from the GUI or CLI. Settings will not be upgraded from previous versions.

The affected models include:

- FGT-40F/FWF-40F and variants
- FGT-50G/FWF-50G and variants
- FGT-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)
- FGT-70G/FWF-70G and variants
- FGT-90G and FGT-91G

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI, and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

On these FortiGate models, consider migrating to using IPsec Dialup VPN for remote access.

See SSL VPN to IPsec VPN Migration for more information.

FortiGate models not listed above will continue to support Agentless VPN (formerly SSL VPN web mode). However, SSL VPN tunnel mode is not longer supported on any models.

2 GB RAM FortiGate models no longer support most FortiOS proxy-related features

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, FortiOS no longer supports most proxy-related features.

However FortiOS 7.6.5 brings back proxy-based inspection for email protocols on FortiGate models with 2 GB RAM. This covers the following services:

- SMTP(s)
- POP3(s)
- IMAP(s)

- NNTP

Firewall policies can once again support proxy-based inspection mode when users select one or more of the above services in the firewall policy.

This change impacts the FortiGate 40F, 60F, and 50G series devices, along with their variants.

See Proxy-related features no longer supported on FortiGate 2 GB RAM models for more information.

2 GB RAM FortiGate models no longer support Security Rating and Security Fabric topology

To enhance the stability of physical FortiGate devices devices with 2 GB RAM, the Security Rating feature and Security Fabric topology visibility have been removed. These changes prioritizes device stability and mitigate potential performance issues. For more information, see Optimizations for physical FortiGate devices with 2 GB RAM.

Policy check required for hairpin traffic

In FortiOS 7.6.5, the default setting for `allow-traffic-redirect` and `ipv6-allow-traffic-redirect` changed from `enable` to `disable`:

```
config system global
  set allow-traffic-redirect disable
  set ipv6-allow-traffic-redirect disable
end
```

Upon upgrade, both of these settings will be changed to `disable`, even if they were enabled before.

Disabling this setting ensures that hairpin traffic arriving at an interface and redirected out on the same interface requires a firewall policy to explicitly allow the traffic. If you want to redirect traffic without the need for a policy based only on routing decision, then manually enable these settings.

Changes in CLI

Bug ID	Description
978171	The NP7 session accounting interval range is now 1 to 600 seconds. Increase the per-session accounting interval to reduce bandwidth usage: `config system npu` `  set session-acct-interval <seconds>` `end` New options to control the bandwidth allowed for traffic flow between NP7 processors and the internal switch fabric (ISF). In some high-traffic configurations, limiting this bandwidth can improve performance, for example by reducing DSW drops and ReasmFails: `config system npu` `  set sw-np-rate <rate>` `  sw-np-rate-unit {mbps | pps}` `  sw-np-rate-burst <burst-rate}` `end`
979401	Add IPv6 address pool support in explicit proxy policies: `config firewall proxy-policy` `  edit <id>` `  set poolname6 <name>` `  next` `end`
1083204	You can enable the following option to add all multicast traffic denied by a firewall policy to the session table: `config system settings` `  set ses-denied-multicast-traffic enable` `end` Enabling this option can affect CPU usage since the software needs to maintain more sessions in the session table. However, on FortiGates with NP6 or NP7 processors, you can use the following command to offload denied multicast sessions to NP processors and reduce CPU usage: `config system npu` `  set mcast-denied-ses-offload enable` `end`
1129653	When multi-vdom mode is disabled, hide the settings:

Bug ID	Description
	`config endpoint-control settings` `  set override {enable | disable}` `end`
1153276	If your FortiGate with NP7 processors is terminating VXLAN-over-IPsec connections, you may notice traffic drops during broadcast storms. One cause of the traffic drops could be VXLAN MAC flapping. VXLAN MAC flapping can occur when the FortiGate receives large numbers of packets that flip MAC addresses in the forwarding database (FDB) between local and remote paths. This activity can use excessive CPU resources and can lead to FDB instability. You can use the following command to stop VXLAN MAC flapping: `config system npu` `  set vxlan-mac-flapping-guard enable` `end` When `vxlan-mac-flapping-guard` is enabled, each VXLAN FDB entry records the encapsulation direction when it is first learned and if a later packet tries to flip the same MAC to the opposite direction, the update is rejected. This behavior prevents VXLAN MAC flapping during loops or broadcast storms. You can restore normal VXLAN FDB behavior by disabling this option.
1165701	NP7 traffic anomaly protection for TCP, UDP, and ICMP checksum error detection now includes the option to allow TCP, UDP, and ICMPpackets with incorrect checksums. `config system npu` `  config fp-anomaly` `  set tcp-csum-err {allow | drop | trap-to-host}` `  set udp-csum-err {allow | drop | trap-to-host}` `  set icmp-csum-err {allow | drop | trap-to-host}` `  next` `end`
1172192	The encrypted DNS certificate configuration behavior has been updated. The TLS certificate used by FortiGate for encrypted DNS services is now taken from: `config system dns-server` `  edit <interface>` `  set ssl-cert <certificate_name>` `  next` `end` rather than: `config web-proxy global` `  set ssl-cert <certificate_name>` `end`

Bug ID	Description
	If no certificate is configured under `config system dns-server`, FortiGate automatically falls back to the `config web-proxy global` certificate.
1172818	Enhance the CLI command `diagnose ip router bgp show` to include disabled items as well as the enabled items.
1179439	When captive portal is not enabled, these settings are hidden: `config authentication setting` `set captive-portal-port` `set captive-portal-ssl-port` `set auth-https` `end` To change these settings, first enable captive portal.
1195267	Support IPv6 BGP route dampening by introducing these CLI commands: `config router bgp` `set dampening6 {enable|disable}` `set dampening6-route-map <string>` `set dampening6-reachability-half-life <integer>` `set dampening6-reuse <integer>` `set dampening6-suppress <integer>` `set dampening6-max-suppress-time <integer>` `set dampening6-unreachability-half-life <integer>` `end`
1204059	The CLI attribute `hw-model` has been renamed to `hw-version` under `config firewall address` for device identification dynamic addresses.
1219353	The `intra-vap-privacy` setting has been removed from `local-bridging vap`.
1220299	In Agentless VPN settings, when multiple domains in dns-suffix are configured, parse each entry separated by ";".
1222523	The FortiGate 120G and 121G port17 to port24 interface speed can be changed to 100Mbps. To operate these interfaces as 100 Mbps interfaces, you must use 100 Mbps Serial Gigabit Media Independent Interface (SGMII) transceivers. You can use the following command to change the speed of the port-17 to port24 interfaces: `config system interface` `edit port17` `set speed {auto | 1000full | sgmii-100full | sgmii-auto}` `next` `end`
1238936	The SFP speed detect CLI option has been updated, replacing auto-module with detect-by-module for improved clarity.

Bug ID	Description
1242593	Added enforce-preferred-source BGP neighbor option to ensure the BGP session source IP (update-source) is used as the preferred source for IPv4 routes learned from the neighbor. This prevents incorrect source IP selection when egress interfaces are unnumbered. `config router bgp` `  config neighbor` `  edit <neighbor-ip>` `  set enforce-preferred-source {enable | disable}` `  next` `  next` `end`
1252864	Supports file encryption on SCP config backups: `scp -OT admin@<FGT_IP>:encrypted-config:<encryption_password> <dst file>`

Changes in GUI behavior

Bug ID	Description
1112727	On a new installation, users logging into the GUI are directed to the FortiCare registration dialog. This dialog ensures users remember to register their device with FortiCare. This feature is supported on the FortiGate 50G, 70G, 90G, 120G, 200G, 700G, 900G and variants.
1158355	In LDAP configurations in the GUI, default to using STARTTLS, and hide the option to disable secure connection. Disabling secure connection can still be done in the CLI. Upon upgrade from an older release, if secure connection is disabled, it will remain disabled after upgrade.
1170592	To facilitate configuring proxy arp address ranges for FortiSwitch VLANs, the GUI now supports adding proxy arp address ranges for VLAN type interfaces.
1190308	On IPsec VPN configurations, the GUI will only provide options to set *Auto* or *UDP* for *Transport mode*. UDP is the default setting for static and dialup tunnels, except when FortiClient is selected. To configure TCP transport, use the CLI.

Changes in default behavior

Bug ID	Description
1107163	The default DH groups for Phase1 and Phase2 IPsec VPN tunnels will be updated from 14 and 5 to 20 and 21 when configured from the CLI. Upon upgrade, VPNs that had the default DH group 14 and 5 will be updated to DH groups 14, 20, and 21.
1133038	An SD-WAN passive health-check does not need to be configured for application performance monitoring to work. For example, this is no longer a requirement: `config system sdwan` `  config health-check` `  edit ""1""` `  set detect-mode passive` `  set members 0` `  next` `  end` `end`
1138921	On FortiGates with NP7 processors, the default setting for vlan-lookup-cache has been changed to disable, and the htab-msg-queue mode is now set to dedicated. `config system npu` `  set vlan-lookup-cache disable` `  set htab-msg-queue dedicated` `end`
1147596	Form authentication no longer works without Captive Portal in transparent web mode. For users upgrading from previous versions to version 7.6.4 and employing transparent proxy with form authentication (`http-policy-redirect enable` + `proxy transparent-web`), the following adjustments are recommended to maintain uninterrupted traffic flow, if not already configured: **1.** Set up Captive Portal: `config authentication setting` `  set captive-portal-type {ip | fqdn}` `  set captive-portal-ip <ip>` `end` **2.** Enable Captive Portal on the interface `config system interface` `  edit <interface>` `  set proxy-captive-portal enable`

Bug ID	Description
	next end
1166396	With asymroute-icmp and asymroute6-icmp enabled, ICMP replies are no longer strictly routed back through the same interface they arrived on. If a return route via the incoming interface is unavailable, the system will now choose the best available route instead. This behavior improves reliability and reduces packet drops in asymmetric routing scenarios. `config system settings` `set asymroute-icmp [enable | disable]` `set asymroute6-icmp [enable | disable]` `end`
1173228	IPSec IKEv2 dial-up tunnel no longer installs a default route when no IP can be allocated from the pool. Tunnel is now rejected if IP assignment fails, preventing misrouting and connectivity loss.
1176942	When `auth-ike-saml-port` is used, iprope will match the local-in traffic only when the destination port is `auth-ike-saml-port` and the destination interface has `ike-saml-server` enabled.
1181737	Added default inclusion of the FortiOS device serial number in the CSR subject (`set csr-include-device-sn enable`). This enhancement ensures SCEP enrollment succeeds in environments that require the `SerialNumber` field, improving compatibility and request validation. `config vpn certificate setting` `set csr-include-device-sn {enable* | disable}` `end`
1204277	The default auto-update schedule for FortiGuard packages has been changed from `automatic` to `daily`.
1207557	When Anycast is enabled, VM license activation now uses dedicated activation FQDNs (vmactivation1/2/3.fortinet.net) instead of general update FQDNs, resulting in faster and more reliable activation.
1221373	Configuration revisions are now only available on FortiGate models with a disk. `revision-backup-on-logout` is enabled by default (previously disabled). A new GUI option called *Create a configuration revision on logout* is added under *System > Settings*, corresponding to the CLI option `revision-backup-on-logout`.
1225202	The default setting for `allow-traffic-redirect` and `ipv6-allow-traffic-redirect` has been changed from `enable` to `disable`: `config system global` `set allow-traffic-redirect disable` `set ipv6-allow-traffic-redirect disable` `end`

Bug ID	Description
	Upon upgrade, both of these settings will be changed to disable, even if they were enabled before. Disabling this setting ensures that traffic arriving at an interface and redirected out on the same interface requires a firewall policy to explicitly allow the traffic. If you want to redirect traffic without the need for a policy based only on routing decision, then manually enable these settings.
1230185	Default user authentication settings (config user setting) has changed to enable only HTTP firewall policy authentication and HTTP redirection to HTTPS. Only affects new FortiOS deployments. Firmware upgrades are unaffected. `config user setting` `  set auth-type http  # the only protocol by default` `  set auth-secure-http enable  # option enabled by default` `end`
1233077	FortiGate now by default only shows recommended configurations for IKE proposals in the CLI. This helps administrators more easily define secured and recommended cryptographic algorithms in the VPN configurations that adheres to security best practices. To set your preference for displaying IKE proposals: `config system settings` `  set ike-proposal-visibility [recommended | all]` `end`
1239371	FortiGate operating in GovRamp (previously called StateRAMP) mode will use dedicated FortiGuard NTP servers as the default configuration after a factory reset. **Previous Behavior** After a factory reset in GovRamp mode, FortiGate defaulted to the following custom NTP servers: `time-a-g.nist.gov  | 129.6.15.28` `time-b-g.nist.gov  | 129.6.15.29` **New Default Behavior** Following a factory reset, the system now defaults to dedicated FortiGuard NTP servers: `ntp1.fortinetgov.com  | 23.249.63.60/23.249.63.61` `ntp2.fortinetgov.com  | 23.249.63.62/23.249.63.63`
1240706	In NGFW policy-based mode, traffic may be bypassed when the IPS engine is not running such as when FortiGate first boots up, the IPS engine is upgrading or when it is manually stopped with debug commands. Instead, NGFW policy mode VDOMs will now drop traffic when IPS sockets are not available."

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>1244317</td><td>Inline IPS is now disabled by default. Previously, inline IPS was enabled by default. Administrators who require inline IPS must explicitly enable it in the IPS settings.

<pre>config ips settings
    set proxy-inline-ips enable
end</pre></td></tr>
<tr><td>1245249</td><td>Additional commands are allowed before device registration to accommodate users that require configuring the device for central management, ZTP and LTP.
Commands added:
<table><tr><th>Command</th><th>Description</th></tr><tr><td>config firewall policy</td><td>Configure IPv4/IPv6 policies.</td></tr><tr><td>config router setting</td><td>Configure router settings.</td></tr><tr><td>config router static</td><td>Configure IPv4 static routing tables.</td></tr><tr><td>config router static6</td><td>Configure IPv6 static routing tables.</td></tr><tr><td>config system admin</td><td>Configure admin users.</td></tr><tr><td>config system central-management</td><td>Configure central management.</td></tr><tr><td>config system dns</td><td>Configure DNS.</td></tr><tr><td>config system interface</td><td>Configure interfaces.</td></tr><tr><td>config system pppoe-interface</td><td>Configure the PPPoE interfaces.</td></tr><tr><td>config system settings</td><td>Configure VDOM settings.</td></tr></table></td></tr>
</table>

Changes in default values

Bug ID	Description
1115026	When configuring a new VPN from the CLI, the default IKE version will be defaulted to IKEv2. `config vpn ipsec phase1-interface` `edit <tunnel>` `set ike-version 2` `next` `end` Upgrading from previous version will not change the IKE version.
1117660	In an access proxy virtual host, add a new default host-type option for fqdn, where the defined host will match sub-domains. `config firewall access-proxy-virtual-host` `edit <vhost>` `set host <string>` `set host-type {sub-string | wildcard | fqdn*}` `next` `end` For example, the host test.com will match vhost1.test.com, but will not match test.com.vhost1.
1118690	On a hyperscale FortiGate, the default values for IPv4 and IPv6 high and low session quotas have been updated. For both session types the high threshold is now 64000, and the low threshold is now 51200. These session quoas are set using the following options: `config system npu` `set ipv6-prefix-session-quota {disable | enable}` `set ipv6-prefix-session-quota-high <high-threshold>` `set ipv6-prefix-session-quota-low <low-threshold>` `set ipv4-session-quota {disable | enable}` `set ipv4-session-quota-high <high-threshold>` `set ipv4-session-quota-low <low-threshold>` `end`
1138491	The number of FortiToken Cloud (FTC) tokens included has been increased from 2 to 3. Additionally, the validity period is no longer limited to one month. FTC tokens are now valid as long as the associated FortiGate has an active support contract.
1166827	For high-end FortiGate (2U+) models, newly created or system-defined webfilter profiles on burn-ROM devices or after a factory reset now enable the error-allow option by default. This corresponds to the GUI setting 'Allow websites when a rating error occurs' and ensures traffic continuity during FortiGuard rating errors. Existing profiles remain unchanged after upgrade.

Bug ID	Description
1182788	IPsec default proposal and DH groups of phase1-interface and phase2-interface have changed: • Remove xxx-SHA1 from default proposal. • Replace default DH groups 5 and 14 with 20 and 21 when configured from CLI.
1200360	The quarantine option is now disabled by default when creating tunnel-mode SSIDs, preventing automatic creation of unused quarantine VLANs and simplifying configuration and management.
1214925	The default value for `update-ffdb` under `config system fortiguard` has been changed from `enabled` to `disabled`. This setting controls whether the FortiGate automatically updates the Internet Service Database (ISDB). With the new default of disabled, ISDB updates will not occur automatically, unless explicitly enabled by administrators.
1248524	The default MTU for IPsec tunnel interfaces has been changed from 1420 to 1402 on the following FortiGate models: FG-5xG, FG-7xG, FG-9xG, FG-12xG, FG-20xG, FG-40xF, FG-60xF, FG-70xG, FG-90xG, FG-100xF, FG-180xF, FG-260xF, FG-300xF, FG-320xF, FG-350xF, FG-370xF, FG-420xF, FG-440xF, FG-480xF, FG-7000F, FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-ARM64-XEN, FG-VM64, FG-VM64-ALI, FG-VM64-AZURE, FG-VM64-AWS, FG-VM64-GCP, FGVM64-HV, FG-VM64-IBM, FG-VM64-XEN, FG-VM64-KVM, FG-VM64-OPC

Changes in table size

Bug ID	Description
1132879	Increase `extension-controller.extender` size for FGT-200G and higher end to 512 to support more lan-extension connections.
1141922	The per-VDOM table size for `firewall.internet-service-custom` has been updated to align with `firewall.service.custom`. The new limits are: 1024 for entry-level models, 2048 for models ranging from 100 to 500, 4096 for 500 to 1500D and for VM4, 10240 for 1500D to 3950B, 32768 for high-end models.
1156114	The maximum tunnel limit configurable for GTP profiles and global GTP settings has been increased from 16,000,000 to 50,000,000.
1190678	The table size limits for `user.group:member` and `user.local` on HighEnd FortiGate models have been increased, with `user.group:member` raised from 3000 to 35000 and `user.local` expanded from 5000 to 35000, improving scalability for large deployments.
1199463	The global table size for `system.external-resource` has been updated from 512 entries to a memory-based capacity, removing the fixed global limit.
1204202	Increase per-vdom limit for `router.route-map` from 256 to 512.
1232017	Increased the maximum table entry limits for ZTNA and access proxy objects to improve scalability for larger customer deployments. The `max_table_entry_vd` has been increased from 256 to 4096 and the `max_table_entry_gl` from 512 to 4096 for the following tables: ztna.destination, ztna.web-proxy, ztna.traffic-forward-proxy, ztna.web-portal, ztna.web-portal-bookmark, and firewall.access-proxy-virtual-host. This change allows significantly higher numbers of ZTNA and access proxy configurations per VDOM and globally.

New features or enhancements

More detailed information is available in the New Features Guide.

Cloud

See Public and private cloud in the New Features Guide for more information.

Feature ID	Description
1152395	FortiGate now supports Multus CNI for Kubernetes connectors, ensuring all IP addresses, including those configured at runtime, are accurately retrieved and added to firewall address dynamic objects, enhancing network security integration.
1196514	FortiGate VM now displays Last Check and Check Due fields, allowing administrators to track remaining time in the license grace period before shutdown. This is especially valuable in air-gapped or denied, degraded, intermittent, or limited (DDIL) environments where connectivity to FortiGuard or FortiManager may be limited, helping prevent unexpected service disruption.

GUI

See GUI in the New Features Guide for more information.

Feature ID	Description
945633	Added GUI visibility for FortiSwitch 802.1X authenticated clients through a new monitoring widget. Enhanced the 802.1X configuration dialog with an Open Authentication option and improved security mode selection using descriptive radio buttons.
1042756	The FortiGate can now detect and display CISA Known Exploited Vulnerabilities (KEV) of FortiClient devices managed by FortiClient EMS. This information can be displayed from the GUI in the Asset Identity Center and in the Assets & Identities widget. Drilling down will display the details of the vulnerability.
1106014	Introduces a redesigned, tabbed settings interface and a flexible theme system that supports custom colour schemes and visual identifiers. Administrators can now personalize their own theme, enabling clearer environment distinction, improved usability, and stronger security awareness in multi-classification deployments.

Feature ID	Description
1176823	Adds GUI support for HA operations that were previously available only via CLI, including resync, failover, and diagnostics. Provides visual HA health details and a config diff view, making it easier to monitor status and identify configuration mismatches directly from the GUI.
1179345	Enhanced the routing configuration by adding GUI support for route-map-out-preferable and route-map-out6-preferable, which were previously only configurable via CLI.
1183975	The FortiGate setup wizard includes options to configure a gateway to establish internet connectivity, which is required for successful registration with FortiCare. Additionally, for air-gapped environments, the wizard allows users to upload an offline license file directly, enabling successful registration even when the device cannot reach FortiCare. This enhancement resolves setup-blocking issues and improves deployment flexibility.
1198079	The dashboards and monitors under the *Dashboard* navigation menu are now consolidated into the following main sub-menus: • Status • Asset and Identities • Network Monitor • FortiView • WiFi Some sub-menus consist of multiple tabbed pages to display data in either a grid format or full monitor format. Admins can still create and customize their own dashboards and add tabs to their dashboards. In the CLI, the `gui-dashboard` subtable of `system.admin` has been removed. Instead a new `system.gui-dashboard-collection` table has been added and referenced by `system.admin`. Upon upgrade, admins will see `gui-dashboard` related errors when running `diagnose debug config-error-log read`.
1251103	Enhances the Security Fabric Physical and Logical topology pages with a new GUI design that lazily loads and renders topology data. This enhancement improves performance and scalability for large fabrics by distributing data retrieval across devices and reducing memory load on the root FortiGate.

HA

Feature ID	Description
1104731	Adds support for selecting a specific source-IP or source-interface for FGSP heartbeat/sync traffic over L3, preventing packet loss caused by ECMP path divergence.
1151108	A new `config system standalone-cluster` CLI option `session-sync` has been added to FortiOS Carrier, allowing users to disable IP session synchronization while continuing to sync GTP tunnels across FGSP peers. This reduces sync overhead and improves performance in carrier-grade environments.

Feature ID	Description
1155614	Hyperscale HA hardware session synchronization improves support for policy based routing (PBR) session failover. To achieve this improvement, HA hardware session synchronization adds PBR-corrected reverse-path information to hardware synchronized sessions. Previously, PBR hardware synchronized sessions were not corrected. Because of this, if your hyperscale FortiGate used policy routing, after a failover, HA hardware sessions would have to re-learn PBR reverse-path information. This re-learning would delay failover for PBR sessions.
1167903	HA now supports synchronizing IPv6 multicast routes from primary to secondary, ensuring that IPv6 multicast traffic have minimal disruption during an HA failover.
1223283	Add support for using softwareswitch member interfaces as HA monitor interfaces. Previously, these interfaces could not be monitored. This enhancement improves configuration flexibility and enables more reliable failover using existing interface layouts.
1228024	Enhances FGSP behavior by synchronizing authenticated firewall users and their active sessions between peer FortiGates. During failover, existing authenticated users are preserved on the peer device, preventing mass re-authentication and ensuring seamless access continuity.
1252380	Enhances HA monitoring by allowing interfaces to be grouped and monitored collectively. Customers can now define failover behavior based on group status instead of individual interfaces, improving stability in complex topologies and reducing unnecessary failover events.
1256231	Enhances the CLI prompt to display the current HA role (e.g., active/passive) of the device. This removes the need for additional status commands and automatically updates after failover, making role identification faster and more intuitive for users.

Hyperscale

Feature ID	Description
1212583	On FortiGates licensed for Hyperscale firewall, the following new options are available to improve control over timers related to Endpoint Independent filtering (EIF) sessions. EIF is also called full-cone NAT. `config system npu` `set eif-tcp-refresh-dir {both | outgoing | incoming}` `set eif-udp-refresh-dir {both | outgoing | incoming}` `set eif-tcp-ttl <time>` `set eif-udp-ttl <time>` `set extra-timeout-tcp <time>` `set extra-timeout-udp <time>` `end`

LAN Edge

See LAN Edge in the New Features Guide for more information.

Feature ID	Description
621730	Switch controller now supports energy-efficient Ethernet (EEE) advertisement and control via LLDP on FortiSwitch, allowing customers to broadcast energy-efficient Ethernet capabilities across the network.
853558	Switch controller now supports pushing custom commands after any configuration change on FSW, including differential updates. This ensures better alignment with specific deployment scenarios and improves system responsiveness.
873384	Introducing MAC move support in the switch-controller to handle client reauthentication when devices reconnect through different ports. This feature improves flexibility and reliability in dynamic network environments, especially with hubs or IP phones.
1101097	Added FortiGate switch controller capability to configure private-data-encryption for managed FortiSwitches. This allows FortiGate to push RADIUS and TACAC+ secrets to FortiSwitches using encoded keys which can be decrypted with the shared private-data-encryption key.
1106711	The FortiSwitch controller now supports generalized Layer 3 switch configuration for hybrid L2/L3 networks. This includes Switched Virtual Interface (SVI), Routed Virtual Interface (RVI), Virtual Routing and Forwarding (VRF), DHCP Server (with minimal configuration for isolated L2 domains), and IPv4 static routes, enhancing network management capabilities.
1117537	Enhancements to the FortiGate-managed FortiSwitch interface deliver improved diagnostics, streamlined grouping actions, and clearer visibility into switch capacity. The topology view is also refined to provide a more intuitive and efficient network management experience.
1127358	Introducing an Advanced Switching Features toggle under System > Feature Visibility. When enabled, it unlocks the LLDP Profile, QoS Policy, VLAN Policy, and PTP Profile tabs on the FortiSwitch Port Policies page, providing enhanced configuration options.
1138430	The maximum length allowed for managed FortiSwitch names has been increased from 16 to 35 characters, enabling customers to use more detailed and descriptive names for better network device management and organization.
1140879	Adds 802.1X per-port client limit support on the switch controller, allowing administrators to cap the number of authenticated sessions per port for improved access control.
1141074	A new CLI command, `set bounce-intf-upon-failover enable`, has been introduced to improve manual failover behavior in VWP A/P FortiGate deployments with wildcard VLANs. When enabled, this command ensures that all monitored interfaces, including members of aggregate interfaces, are explicitly brought down during failover on the secondary unit. This enhancement addresses a previous limitation where only the native VLAN received gratuitous ARPs, leaving non-native VLANs unaware of the failover event. `config system ha` `  set bounce-intf-upon-failover {enable|disable}` `end`

Feature ID	Description
1144109	Adds support for automated FortiAP location determination using userdefined coordinates, onboard GPS, or WiFi RTTbased trilateration. Provides accurate AP positioning for regulatory compliance and simplifies deployments where manual or GPS data is unavailable.
1150128	FortiGate-managed PoE FortiSwitch ports now support configurable maximum power settings. Users can choose between 30W, 60W, or class-based modes, allowing greater flexibility to meet the power needs of connected devices.
1151101	Added a 6GHz channel utilization chart for FAP G and K series models on both the *Managed FortiAPs* page and on the *Dashboard > WiFi > FortiAP Status* widget. Users can now also customize the layout of channel utilization charts for better visibility and control.
1152960	FortiLink now supports pushing trusthost settings for admin accounts on managed FSWs, enhancing network security by restricting access to specific IPs.
1153434	Adds support for stacking up to four FSW units and exposing them as a single aggregated entity. This enhancement simplifies management by presenting one unified system instead of multiple individual FSW units, improving clarity and operational efficiency.
1154361	FortiLink now ensures LLDP PDUs are sent reliably, even when over 1000 VLANs are configured, improving network stability and device discovery in large-scale deployments.
1174644	FortiGate now supports managing more FortiSwitch units - 50G variants increased from 8 to 16, 200G from 64 to 96, and 2600F from 196 to 300, enhancing scalability for larger deployments.
1185772	Default soft-switch interfaces and open SSIDs have been removed across FortiWiFi platforms to enhance security and simplify network design. For 4xF/6xF/G-series models, the default WiFi VAP remains in tunnel mode with preconfigured IP, DHCP, and firewall policies for easy setup. On 8xF-2R models, WiFi VAPs now operate in bridge mode, integrating with the hardware switch so clients receive DHCP from the internal interface and benefit from firewall policy control.
1187026	Mesh leaf FAP settings can now be configured directly through the GUI, enabling faster, more intuitive setup of mesh connections.
1194146	Adds 802.1X, MAB, and Dynamic VLAN support to the FortiGate software switch, enabling authenticated access control and intra-switch policies to regulate traffic.
1196410	Layer 3 Access Control Lists (ACLs) in FortiAP now support Fully Qualified Domain Names (FQDNs) and simple wildcard matching for both source and destination addresses, expanding beyond the previous limitation to static IP addresses only. This enhancement improves configuration flexibility for dynamic and cloud-based environments by eliminating the need to manually track changing IP addresses.
1200877	Add LoRaWAN gateway support to the FortiAP 222KL, enabling the device to receive LoRaWAN sensor data and securely forward it to supported network servers. This enhancement allows the AP to operate as both a WiFi and LoRaWAN gateway, streamlining IoT sensor integration within existing network environments.

Feature ID	Description
1201086	This update introduces two new DARRP profilesarrp-default-high-density and arrp-default-medium-densityallowing users to choose a profile aligned with their deployment environment. Weight-setting ranges are refined (maximum reduced to 200), and default weight values for the rogue AP, weather channel, and DFS channel have been adjusted to enable more realistic and effective channel assessment.
1211127	WiFi controllers now process the RADIUS Filter-ID attribute during 802.1X authentication to automatically map clients to existing user groups. This enhancement triggers the creation of WSSO firewall authentication entries, ensuring the correct firewall policies are applied immediately without requiring additional user login steps.
1212557	Add support for configuring IGMP snooping static groups on managed FortiSwitch through FortiGate. This enhancement allows administrators to define static multicast group entries, providing improved control and predictability in multicast environments.
1217645	Previously, virtual switches in a software switch could not enable 802.1X authentication. Now, this restriction is removed, and 802.1X can be enabled when the software switch's `intra-switch-policy` is set to `explicit`, allowing secure dynamic VLAN control and traffic regulation.
1219931	Adds a new highpse option that allows administrators to enable 802.3af PoE output on the LAN3 PSE port when the FAP23JK is powered via 802.3at. This provides greater flexibility by allowing the FAP23JK to power another device in scenarios where PoE output was previously disabled.
1227507	Support multiple geneve interfaces with the same underlying physical interface to be members of same software switch.
1238935	Adds support for defining trunk portselection criteria at the global switchcontroller level on Marvell platforms. Centralizing this configuration replaces the previous pertrunk approach.
1244920	Adds the ability to enable both Dynamic VLAN and VLAN Pooling simultaneously when configuring a VAP with RADIUS authentication. This enhancement expands flexibility in enterprise deployments by allowing VLAN assignment from RADIUS or, when absent, falling back to the local VLAN pool for seamless segmentation.
1244925	Enhances VLAN pooling in WTP group mode by allowing multiple WTP groups to be selected when creating a VLAN entry. This improves flexibility and scalability for environments where VLAN pools must span several WTP groups.
1249992	Enables MultiLink Operation (MLO) on Local Standalone VAPs for FortiAPK models, extending WiFi 7 MLO capabilities beyond Managed FortiAPs. Authentication is handled directly on the FortiAP, allowing full MLO functionality even when operating independently.

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description
1042710	A new summary panel has been added at the top of the Log Details slide, showing log timestamp, policy info, and a concise overview of security events with hover-enabled tooltips and quick actions.
1124108	Introduce support for custom log formats to the syslog server using log custom-format and log-template configurations. Previously, FortiGate sent logs only in fixed formats (CSV, CEF, RFC 5424, JSON). With this enhancement, customers can fully tailor syslog output to match the exact requirements of their external logging system.
1156113	Adds secure SFTP support and standard LZ4 log compression to FortiGates logupload feature, expanding beyond the previous FTPonly implementation. The update improves log transfer security and flexibility while supporting both default FLZ4 and industrystandard LZ4 formats.
1170883	In *Log Settings > Global settings* under *Preferences*, when *Resolved hostnames* is enabled, provide 2 options: • *On log creation* (resolve-ip enabled) will add the resolved hostname when the logs are generated and add it as dstname. In the GUI, display the dstname field. • *When viewed* (resolve-hosts enabled) will resolve the destination IPs during fetching of logs. If both are enabled from CLI, then *On log creation* takes precedence.
1179741	Improves TACACS+ accounting logs by adding full CLI change details to the reason field, providing more complete event log entries for external audit systems.

Network

See Network in the New Features Guide for more information.

Feature ID	Description
1040534	Enables synchronization of fullcone NAT expectation sessions within FGSP and FGCP clusters. This ensures peertopeer UDP traffic behind CGNAT remains accessible across all cluster members.
1058743	Auto speed negotiation on the 10G Base-T interface now allows the 1G/10G copper ports on the FGT100xF to automatically handle both 1G and 10G speeds and duplex settings, eliminating the need for manual adjustments and enhancing user experience.
1061102	Fabric Overlay Orchestrator now supports IPAM integration, enabling the overlay orchestrator to utilize IPAM for Hub and Spoke overlay network and spoke LAN addressing scheme.
1076320	Introducing improved hashing for NP7-offloaded GRE tunnels that considers inner L3/L4 headers, enabling ECMP offload over loopback and balanced traffic distribution across LACP members. This enhancement boosts throughput and load efficiency in GRE deployments. CLI Changes: Configure the LAG hashing algorithm for NP7 GRE sessions:

Feature ID	Description
	`config system npu` `set lag-hash-gre {disable | gre_inner_l3 | gre_inner_l4 | gre_inner_l3l4}` `end` Choose from: • `disable`: Disable GRE inner header information as hash input for LAG. • `gre_inner_l3`: Use GRE inner L3 header information as hash input for LAG. • `gre_inner_l4`: Use GRE inner L4 header information as hash input for LAG. • `gre_inner_l3l4`: Use GRE inner L3 and L4 header information as hash input for LAG. Enable the configured NP7 GRE hashing algorithm for a LAG: `config system interface` `edit <name>` `set type aggregate` `set algorithm NPU-GRE` `next` `end` Enable multiple path support for NP7 GRE sessions over software loopback interfaces: `config system gre-tunnel` `edit <name>` `set loopback-ecmp-offload {disable | enable}` `next` `end` Choose from: • `disable`: Disable multi-tunnel offloading support. • `enable`: Enable multi-tunnel offloading support.
1095610	You can now configure ip6-link-local directly under an interfaces IPv6 settings. When a manual linklocal address is applied, the system automatically removes the default automatically-generated IPv6 linklocal address, preventing multiple linklocal addresses from coexisting.
1099374	If your FortiGate with NP7 processors is experiencing high CPUusage because the CPU is processing many denied sessions, you can use the following command to offload those denied sessions to NP7 processors and reduce CPU usage: `config system npu` `set session-denied-offload {enable | disable}` `end`
1102585	Introducing a new IPAM type firewall addresses, enabling automatic IP range allocation to VPN clients across multiple FortiGates. This allows centralized IP management and traffic control across distributed subnets, improving scalability and operational efficiency.

Feature ID	Description
1122263	FortiOS now supports IPv6 PCP for DNAT46, enabling inbound PCP MAP requests in NAT64 deployments. This enhancement allows FortiGate to dynamically manage IPv6-to-IPv4 mappings via PCP, improving compatibility with CLAT-based CPEs.
1124535	FortiGate now provides control over whether domains from delegated IPv6 prefixes are included in DNS Search List (DNSSL) options sent via Router Advertisements. This feature improves flexibility in managing domain propagation for downstream clients. `config ip6-delegated-prefix-list` `edit <id>` `set dnssl-service {enable | disable}` `next` `end`
1125884	Adds support for displaying Forward Error Correction (FEC) status, RX/TX bits per second (bps), packets per second (pps), and host-level RX drop statistics in NIC interface diagnostics, providing enhanced visibility to assist with debugging and performance analysis.
1130037	Add support for VXLAN Anycast Gateway, EVPN IRB, and Type-5 EVPN routes, enabling seamless L2/L3 service integration and scalable IP prefix advertisement across the VXLAN fabric. It simplifies mobility and routing in modern data center deployments.
1130044	Adds DHCP template support, allowing interfaces to inherit DHCP settings from reusable templates. This introduces a new DHCP Template table and extends DHCP server attributes to support template-based configurations. IPAM rules and interfaces can now reference a DHCP template, enabling consistent and scalable DHCP configuration across interfaces.
1130607	FortiGate now supports 802.1p CoS marking (cos0cos7) for locally generated ARP packets, allowing customers to align ARP traffic with network QoS policies and constraints.
1135789	IPv6 support has been added to the in-band management IP feature, enabling HA members to be accessed via IPv6. This provides greater flexibility and future-proofing for networks transitioning to IPv6.
1136781	BGP neighbors can now be assigned a name that appears alongside their IP address in the GUI and logs. This improves readability and simplifies peer identification in large or multi-tenant environments.
1137933	FortiGate now supports BSR (Bootstrap Router) for IPv6 multicast, enabling dynamic RP discovery for large-scale deployments and aligning IPv6 capabilities with existing IPv4 PIM BSR support.
1138542	PIM now supports all VRFs (up to 511) and is aware of IPv6 multicast routing and forwarding over a single overlay, enhancing network scalability and flexibility compared to the previous VRF 0-only support.
1141346	FortiGate Rugged (FGR) now supports acting as an MQTT broker, allowing users to send MQTT protocol messages from onboard IoT sensors and systems to a central collection platform. This enhancement enables publishers and subscribers to communicate via the FGR broker, enabling greater network scalability.
1149106	FortiOS now supports upstream SSL for HTTPS virtual servers. When enabled, FortiGate

Feature ID	Description
	converts incoming HTTP traffic to HTTPS between itself and the HTTPS server, improving security for trusted internal deployments with resource-constrained devices.
1154356	FortiGate integrates BBR (Bottleneck Bandwidth and RTT), a model-based TCP congestion control algorithm developed by Google, offering significantly improved data transmission speeds under congested network conditions compared to the traditional CUBIC method.
1157379	FortiOS introduces AI- and ML-powered capabilities that detect malicious activities within DNS traffic. This enhances security by identifying potential DNS tunneling attempts used for data exfiltration or command-and-control. Additionally, FortiOS now includes a domain whitelist within the machine learning database, allowing wellknown and trusted domains to be exempt from detection, reducing false positives and improving detection accuracy.
1158738	The maximum item for `set-aspath` in BGP route maps has been increased from 79 to 255 characters. This allows support for longer AS path prepending, enabling advanced self-healing configurations in large-scale networks.
1158740	FortiGate adds support for graceful BGP shutdown (RFC 8326) to allow controlled and orderly shutdown of BGP sessions. This ensures peers have time to adjust to the change and lower the local preferences of the routes associated with the graceful shutdown community and prefix. CLI: `config router bgp` `  config neighbor` `  edit <IP address>` `  set shutdown {enable | disable | graceful | graceful-soft}` `  set graceful-shutdown-community <community>` `  set graceful-shutdown-local-preference <local preference>` `  set graceful-shutdown-delay <delay>` `  next` `  end` `end`
1168598	FOS now extends session helper statistics beyond SIP to include FTP, TFTP, RTSP, and PPTP protocols, enhancing visibility and troubleshooting for these traffic types via CLI.
1184721	Support for GPON transceivers has been added to FortiGate with SFP/SFP+ ports, enabling deployment in fiber-based access networks. This enhancement allows customers transitioning from legacy DSL infrastructure to adopt widely used GPON technology, improving interoperability and easing migration.
1198566	FortiOS now adds ingress interface and VLAN ID as additional session keys for multicast traffic in Virtual Wire Pair configurations with `wildcardvlan` enabled. This enhancement enables the FortiGate to create distinct multicast sessions for traffic returning through the same VWP on different VLANs, improving accuracy and ensuring optimal session handling.
1203525	Previously, MAC addresses authenticated via MAC Authentication Bypass (MAB) were stored as static, non-expiring authorized entries. The new feature adds support for creating dynamic authorized MAC entries, allowing them to age out naturally and ensuring proper deauthorization.

Feature ID	Description
1206938	Introduces port setting override for single MAC match control and upgrades match period resolution to hours. NAC ports now support QoS policy actions and full PoE configuration, giving customers greater control and flexibility in managing matched endpoints.
1207338	Adds support for the negation in Cisco ACI direct connector address object filters, including new L3OutSubnetDescription and L3OutSubnetNameAlias filters with full IPv4/IPv6 compatibility. This enhancement simplifies filtering by allowing administrators to exclude specific subnets instead of enumerating all included ones, improving usability in environments with many networks and few exceptions.
1212772	By default, changes to outbandwidth or egress shaping profiles on a physical or VLAN interface do not take effect for IPsec tunnels or sessions that are already established and offloaded by NP7 or NP7Lite (SOC5) processors. To apply the updated egress shaping settings, you must flush or reinstall the affected IPsec SAs and clear any offloaded sessions. Doing this rebuilds the IPsec tunnel and associated sessions using the new interface shaping configuration. For FortiGates with NP7Lite (SOC5) processors, you can use the following command to cause FortiOS to automatically flush or reinstall the affected IPsec SAs and clear any offloaded sessions after changing the configuration of an outbandwidth or egress shaping profile: `config system npu` `  set mcs-auto-start enable` `end` `mcs-auto-start` is disabled by default.
1215201	Adds support for an external active GNSS antenna on FWF50G5G, extending the existing GPS feature to enable stronger signal reception. This enhancement improves GPS accuracy and reliability in environments where the built-in passive antenna is insufficient.
1215886	Add a new setting that functions like strict Reverse Path Forwarding checks for reply packets. `config system settings` `  set src-check-reply {enable | disable}` `end` Where: • `enable`: Enable source verification for reply packets. • `disable`: Disable source verification for reply packets (default).
1223803	Introducing customizable DHCP Option 82 configuration, enabling administrators to select any combination of sub-options and define a custom delimiter. It replaces the previous configuration of only three fixed, non editable styles.
1230743	Adds support for CoS marking on locally generated DHCPv4 and DHCPv6 client packets. This enhancement enables FortiGate to obtain IP addresses from service providers that require CoSmarked DHCP requests.
1237854	Support configuring next-hop modification for VPNv4 and VPNv6 routes on route reflectors by introducing these CLI commands:

Feature ID	Description
	config router bgp config neighbor edit <name> set next-hop-self-rr-vpnv4 {enable|disable} set next-hop-self-rr-vpnv6 {enable|disable} next end end
1239128	Adds dynamic BGP-based learning for selected ISDB categories, specifically Botnet and Spam, allowing FortiGate to automatically receive and advertise these IPs for more responsive, threat-aware routing.

Operational Technology

See Operational Technology in the New Features Guide for more information.

Feature ID	Description
1116708	Adds MACsec support across all applicable FortiGate Rugged (FGR) models with hardware switch. This enables secure Layer2 encryption and meets mandatory compliance requirements for regulated OT environments where MACsec is required.
1179350	Adds a fabric stitch trigger for GPIO status changes in FortiGate Rugged (FGR) when Digital IO triggers are activated. This enhancement allows FGR to execute user-defined stitch actions, such as enabling or disabling specific policies or VPNs based on external switch or button inputs.

Policy & Objects

See Policy and objects in the New Features Guide for more information.

Feature ID	Description
881927	Support key GTPv1 signaling messages on the S3/Gn interface, enabling successful tunnel establishment for 3G users transitioning to 4G/5G networks. This enhancement ensures smooth inter-RAT handovers by correctly recognizing and mapping GTPv1 to GTPv2 messages.
1022061	Support Fully Qualified Domain Name (FQDN) address groups within the Internet Service Database (ISDB), addressing the challenge of frequently changing IP addresses and ensuring accurate and reliable firewall policies.

Feature ID	Description
1035331	FOS now supports dynamic shaping profiles for traffic offloaded by NP7 and NP7Lite (SoC5) processors, allowing traffic control policies to be applied per user based on authentication details and bandwidth parameters from the RADIUS server. This enables flexible QoS strategies tailored to individual users instead of static interface-based shaping.
1078303	FQDN address groups within the ISDB, previously supported in firewall policies, can now also be applied to NGFW policies.
1107413	Support for configuring users and groups in policy routes has been added, allowing administrators to use users and user groups as source filters. This enhancement provides granular control over network traffic, enabling organizations to prioritize resources for specific users or groups.
1129832	FOS now supports IPv6 wildcard addresses in firewall policies, enhancing flexibility, scalability, and ease of management in IPv6 networks.
1132012	Filtering support has been added to mutable policy lists, allowing users to refine policies based on key metrics, such as bytes, packets, hit count, and last user. This enhancement provides more precise control for identifying high-impact or frequently used policies, improving efficiency in policy management and troubleshooting.
1138502	FortiOS Carrier now supports filtering for 12 new Radio Access Technology (RAT) types introduced in 3GPP TS 29.274 Release 17. These new RAT types can be added to RAT timeout profiles using the `config gtp rat-timeout-profile` command. You can also add these new RAT types when configuring GTPv2 policy filtering. The new RAT types are: WB-E-UTRAN(LEO), WB-E-UTRAN(MEO), WB-E-UTRAN(GEO), WB-E-UTRAN(OTHERSAT), EUTRAN-NB-IoT(LEO), EUTRAN-NB-IoT(MEO), EUTRAN-NB-IoT(GEO), EUTRAN-NB-IoT (OTHERSAT), LTE-M(LEO), LTE-M(MEO), LTE-M(GEO), and LTE-M(OTHERSAT).
1141091	Custom tags can now be created and applied to various address types and policy types. This helps administrators organize their addresses and policies, quickly visualize the category and easily filter based on the assigned tags when many addresses and policies are configured.
1159457	A new `telemetry` sub-type has been added to the dynamic firewall address type, along with a new `agent-id` attribute that directly references a FortiTelemetry agent, and a new `telemetry` category for firewall address groups. Previously, FortiTelemetry agents were represented as firewall addresses of type `ipmask`, named after the agents serial number and dynamically updated by telemetryd. This enhancement introduces a more structured and scalable way to define and manage telemetry agents, allowing both individual telemetry addresses and grouped telemetry address objects to be used in telemetry polices, improving clarity, policy targeting, and operational efficiency.
1169071	Manually override and disable passive learning of FQDN addresses by disabling the following command on the firewall address object: `config firewall address` `edit <address>` `set passive-fqdn-learning {disable | enable}` `next`

Feature ID	Description
	end By default, this setting is enabled.
1172871	To enhance user experience, when a new telemetry address is created, it can be automatically added to a default telemetry address group. config telemetry-controller global set auto-group-telemetry-addr {enable* | disable} end

SD-WAN

See SD-WAN in the New Features Guide for more information.

Feature ID	Description
1135850	Added IPv6 support for HTTP and TWAMP protocols in SD-WAN health-checks. Added probe-response in ipv6-allowaccess of interface settings. FGT_A: config system sdwan config health-check edit "ipv6_test" set addr-mode ipv6 set server 2000:172:16:200::1 set protocol twamp next end end FGT_B: config system interface edit "port3" ... config ipv6 set ip6-address 2000:172:16:200::1/64 set ip6-allowaccess ping https ssh probe-response end next end config system probe-response set mode twamp

Feature ID	Description
	`end`
1137030	Spokes can now define per-tunnel egress shaping values that are automatically communicated to hubs during IKEv2 negotiation. Hubs enforce these values instantly with persistent policing, delivering consistent QoS across diverse WAN links without requiring active bandwidth testing.
1156116	Enhancements to SD-WAN interface speed test to allow for dynamic QoS application and more resiliency for cloud speed test connections. **1.** Automatically apply scheduled speed-test result (Out/In Bandwidth) to interface for QoS purpose. Respect any configured min+max in/out bandwidth values. **2.** Select "FTNT_Auto" as default cloud server group to perform speed-test if a specific server group isn't specified. **3.** Initiate retry mechanism once speed-test against cloud server fails.
1157885	ADVPN spoke-to-spoke traffic shaping via IKE bandwidth negotiation. Spokes can now define per-tunnel egress shaping values that are automatically communicated to spokes during IKEv2 negotiation. Spokes enforce these values instantly with persistent policing, delivering consistent QoS across diverse WAN links without requiring active bandwidth testing.
1158737	This enhancement to adaptive FEC introduces the capability to send FEC parity packets in a secondary overlay tunnel that is associated with the same destination. The following setting can be configured on the primary tunnel which requires parity packets to be sent on a redundant tunnel: `config vpn ipsec phase1-interface` `edit <tunnel>` `set fec-separate-redundant-tunnel enable` `next` `end` The redundant tunnel must have the same destination location-id as the original tunnel.
1158739	Adaptive FEC now has the ability to take the TOS/DSCP value into consideration when mapping the FEC profile. In addition, new negate options allow users to match against the negative of a threshold. For example, negate packet-loss of 5% means any packet-loss fewer than 5% will be matched. New CLI: `config vpn ipsec fec` `edit <name>` `config mappings` `edit <id>` `set packet-loss-threshold-negate {enable | disable}` `set latency-threshold-negate {enable | disable}` `set bandwidth-up-threshold-negate {enable | disable}` `set bandwidth-down-threshold-negate {enable | disable}` `set bandwidth-bi-threshold-negate {enable | disable}`

Feature ID	Description
	config tos edit <id> set tos <value> set tos-mask <value> set base <value> set redundant <value> next end next end next end
1158784	Enhance packet duplication to confine packet duplication across multiple dial-up tunnels to the same Spoke. When the same subnet is behind multiple spokes, a Hub device will now use the existing location ID setting to uniquely identify and limit the destination for duplicated traffic. config system settings set location-id <ip> end
1158786	Packet duplication on hub devices can now be configured to automatically activate when a spoke begins sending outofSLA remote health checks. Duplication continues until the hub once again receives inSLA health checks from that spoke. The duplication is limited to the affected spokes tunnels. For each original packet, the hub sends one duplicate per tunnel until either all tunnels have transmitted the same packet or the configured maximum is reached. Hub: config system sdwan set duplication-max-num < value > config duplication edit 1 ... set packet-duplication on-demand ... next end end
1158787	SD-WAN duplication now supports selective member targeting, offering greater flexibility and control. Previously, duplication applied to all members in one zone indiscriminately.
1158788	Duplication rules now support matching traffic based on ToS (Type of Service), enabling more precise control. Previously, ToS criteria were not available in the duplication configuration.
1158789	Introduced an option to allow load-balance service with hash-mode inbandwidth / outbandwidth / bibandwidth to steer traffic based on shared underlay available bandwidth or individual overlay available bandwidth.

Feature ID	Description
	CLI: `config system sdwan` `  config service` `  edit <number>` `  set load-balance enable` `  set hash-mode {inbandwidth | outbandwidth | bibandwidth}` `  set bandwidth-type {overlay* | underlay}` `  next` `  end` `end`
1158790	Utilized bandwidth on the overlays or their underlays will be checked before duplication. If it is less than specified threshold, duplication will start; if it exceeds specified threshold, duplication will stop.
1160119	A new FortiView widget *FortiView SD-WAN application performance* is added which leverages the passive WAN health capabilities of SD-WAN to log and monitor application performance metrics. These metrics are aggregated into five new FortiView report types: **1.** Application performance overview: Overview of different performance metrics of monitored applications. **2.** Application response time: Shows response time of a given application **3.** Application connection stability: Shows application connection stability in terms of jitter **4.** Application retransmission: Shows application traffic packet retransmission **5.** Application reliability monitor: Shows packet loss and abrupt connection termination by tcp reset A new GUI option *Log application health metrics* is added to the firewall policy logging options section to enable the required logging for this widget.
1184491	Sometimes, SD-WAN underlay members have monthly total bandwidth usage limits, which incurs overage costs with their ISPs once the limit is exceeded. To accomplish traffic steering based on monthly traffic volume, volume quota limit, billing start day, and related settings are added to SD-WAN members. If accumulated traffic volume on one member exceeds the specified quota limit within a one-month billing period, the member's cost, weight, or volume-ratio value can be automatically adjusted to force or redirect traffic to other members.
1187158	This feature enables hubs to detect when a spoke is dead (no SLA probes over a configurable duration) and suppress routes to that spoke. A BGP route-map-out is used to match this suppression status, and adjusts the MED to inform BGP peers of the hub to direct traffic to the spoke through another hub. `config system sdwan` `  config health-check` `  edit` `  set update-bgp-route {enable | disable}` `  next`

Feature ID	Description
	`` end end config router route-map edit ""suppress_dead_spoke"" config rule edit 1 set match-suppress enable set set-metric 999 next edit 2 set set-metric 10 next end next end config router bgp config neighbor edit ""172.31.0.129"" // BGP peer sending traffic to spoke through hub set attribute-unchanged med set route-map-out ""suppress_dead_spoke"" next end end ```
1250124	Speedtest scheduling is now coordinated automatically between the FortiGate appliance and the back end Fortinet servers, removing the need to configure retry settings. The use of speedtest results for traffic shaping has also been simplified, with all related settings moved directly into the interface configuration. Speed-test traffic now ignores interface traffic shaping, but is affected by values for update-inbandwidth-maximum and update-outbandwidth-maximum settings when configured within that speed-test's settings.These changes reduce administrative overhead and make speedtestdriven shaping more consistent and easier to manage.

Security Fabric

See Security Fabric in the New Features Guide for more information.

Feature ID	Description
1084590	Add support for sandbox submission exemptions based on AIP/MPIP labels, allowing FortiGate to respect data governance policies and prevent sensitive files from leaving the network. It offers finer control beyond file-type based exemptions.
1109370	Introducing support for simultaneous use of FortiSandbox Cloud and on-premise, enabling AV profiles to route files based on policy or auto-selection. This hybrid approach offers flexible sandboxing, data privacy, and compliance.
1124949	Introducing Fabric Feed, an improvement to the existing external feeds feature, which was formerly known as threat feeds. This update lets FortiAnalyzer upload Fabric Feeds directly to the Cloud AMQP server. Once uploaded, these feeds are automatically synchronized with FortiGate devices linked to the same FortiCare account. This enhancement introduces a centralized, cloud-native approach to distributing feed intelligence, improving operational efficiency and consistency across the Security Fabric.
1145288	FortiGate now supports importing IPv6 addresses from the APIC controller, expanding its capabilities beyond the previous IPv4-only support.
1145292	Introducing support for Cisco ACI external EPG (l3extSubnet) subnets in FortiGates Direct Connector. This enhancement allows automatic import of external EPG subnets for use in security policies, improving integration and policy accuracy.
1145865	Downstream Security Fabric members may now be authorized based on the certificate issuer's CN and the devices subject CN. As long as the issuer is a trusted CA, or one of the CAs in the hierarchy of signing chain is a trusted CA, downstream devices will maintain authorization, even if certificates are renewed, reducing admin reauthorization frequency.
1179342	Adds a VDOM dropdown in the Fabric Central Management GUI for FortiGate devices with multi-VDOM enabled. This enhancement provides a more intuitive configuration experience by allowing VDOM selection directly within the GUI.
1186780	Security Rating tooltips now include a footer button to view all insights for a configuration object, plus individual controls to hide specific insights directly from the tooltip. Hidden insights are still indicated, improving visibility and user control.
1223120	Adds category and popularity filters to the SaaS table and introduces multi-select and bulk add actions. Enables faster CASB profile creation, especially when managing a large number of SaaS entries.

Security Profiles

See Security profiles in the New Features Guide for more information.

Feature ID	Description
983930	A new classification framework lets administrators mark applications as sanctioned or unsanctioned by application or category. Any app not explicitly classified is automatically labeled as unclassified by default, though the implicit rule can be changed to treat them as sanctioned or unsanctioned. This provides clearer visibility in logs and improves monitoring and management of application usage.
1014488	Re-imagining MPIP label integration, this update allows MPIP labels to be used directly with DLP profiles without needing a dictionary. MPIP labels now have their own settings, enhancing usability. Additionally, remote MPIP labels can be synchronized automatically from a Microsoft Purview account through the Azure SDN connector, complementing locally defined labels. This enhancement reduces manual effort, minimizes errors, and improves data protection compliance.
1055921	The inline CASB security profile has been enhanced to support control factors, such as tenant information, in JSON data exchanged between a web browser and a custom SaaS application. For example, for some custom SaaS applications, the URL does not change to reflect the type or identity of the user or organization when logged in because such tenant information is exchanged using JSON data instead of through changes in the URL. With this enhancement, JSON data can be extracted using JQ filters.
1080558	FortiData is a data security product for discovering, classifying, and labeling files with sensitive data within your file storage system. With the integration of FortiData with FortiGate, you can configure FortiGate to pass the fingerprint of transferred files to FortiData for analysis and labeling. The labeling result is then returned and used for DLP processing in FortiGate policies.
1122518	Introducing application control support for GenAI, which includes adding a new database type, AIAP, for GenAI rules. This feature also enhances UTM AppCtrl GenAI logs with new fields: aiuser, model, dcgeo, usecase, cloudgenai, and prompt. Additionally, it introduces a new application category, Generative AI, under *Security Profiles* > *Application Signatures*, and adds two new FortiView types, AI Applications and AI Use Cases. These updates enhance the management and categorization of GenAI signatures, offering improved visibility and insights into AI-related activities.
1149705	Introduces new CLI controls that allow administrators to monitor or automatically block files when outbreakprevention connections to FortiGuard timeout or encounter errors. This ensures that failed requests are visible in logs and can be handled proactively rather than silently failing. `config antivirus profile` `edit <name>` `set outbreak-prevention-error-action {log-only | block | ignore}` `set outbreak-prevention-timeout-action {log-only | block | ignore}` `next` `end`
1154475	Introducing support for FortiSandbox Inline scanning in Flow mode on FortiGate. This enhancement enables customers to utilize sandboxing alongside other Flow-mode features, such as IPS, to improve threat detection capabilities without switching to Proxy mode and to

Feature ID	Description
	streamline security operations.
1156119	Added a new "warning" action to the file filter profile, allowing FortiGate to display a user authorization page before downloading matched file types over HTTP in proxy inspection mode.
1166828	In this enhancement, proxy-based inspection is brought back for email protocols on FortiGate models with 2 GB RAM. This covers the following services: • SMTP(s) • POP3(s) • IMAP(s) • NNTP Firewall policies can once again support proxy-based inspection mode when users select one or more of the above services in the firewall policy.
1171657	Add support for external hash-based lists of URLs and SNIs, for use by web filter profiles, to filter access to hashed list entries. `config system external-resource` `edit "hash"` `set category 192` `set threat-feed-hash-mode {plain-text-db* | hash-db}` `set resource "http://10.1.1.91/ext1"` `next` `end`
1172927	Introducing a new type option for local URL filter tables to enhance URL filtering flexibility. This allows the creation of custom FortiGuard categories using the local URL filter table, applicable in both policy-based and profile-based NGFW modes.
1178045	Add CLI setting to configure the FortiSandbox inline mode block (ILB) timeout: `config antivirus profile` `edit <name>` `set fortisandbox-scan-timeout <30-180>` `next` `end`
1196767	FortiGate now supports TLS 1.3 hybrid Post-Quantum Cryptography (PQC) key exchanges in SSL deep inspection (proxy mode), enabling secure traffic inspection. This enhancement ensures compatibility with modern browsers and PQC-enabled servers that utilize algorithms such as X25519MLKEM768.
1199124	Adds WebSocket traffic inspection, allowing UTM modulesincluding DLP, AV, IPS and FileFilterto detect and block sensitive data, malware, and restricted files sent over WebSocket. With the growing adoption of WebSocket-based applications, this provides essential security coverage previously unavailable.

Feature ID	Description
1203906	Adds classification filters to the Application and Filter Overrides list, enabling admins to block, monitor, allow, or quarantine sanctioned, unsanctioned, or unclassified applications. This provides more granular control over application behavior and improves overall application governance.
1214957	Supports leading agentic AI protocols, including the Model Context Protocol (MCP) and the Agent-to-Agent Protocol (A2A), enabling full detection, visibility, and action under application control. New AI-specific log fields and FortiView enhancements provide deeper insights into AI-driven activity, improving oversight and security for emerging AI workloads.
1219574	Adds support for handling category detection without contacting FortiGuard servers when only local or external threatfeed categories are used in WebFilter profiles (NGFW profile mode), URLcategory policies (NGFW policy mode), or SSL exemptions. This eliminates unnecessary rating traffic and improves performance.

System

See System in the New Features Guide for more information.

Feature ID	Description
1000357	Improved Hyperscale FortiOS support for SNMP MIB OIDs to monitor IP and PBA usage in CGNAT IP pools. The newly supported fields include: • fgFwIppStatsFreePBAs, number of free PBAs in ippool list. • fgFwIppStatsInusePBAs, number of in-use PBAs in ippool list. • fgFwIppStatsTotalPBAs, number of PBAs in ippool list. • fgFwIppStatsInuseIPs, number of in-use IPs in ippool. • fgFwIppStatsFreeIPs, number of free IPs in ippool. The fgFwIppStatsExpiringPBAs SNMP field is not supported by FortiOS 7.6.5.
1006397	Granular failure details for each device in a federated upgrade are now reported, allowing users to identify individual devices with specific failure reasons during the upgrade process.
1058390	Integrate an AI-driven assistant and a CLI Code Lab into FortiGate to provide RAG-enhanced documentation support, automated diagnostic analysis, and CLI script execution. The FortiAI-Assist can answer technical questions using the FortiOS documentation and troubleshoot issues by reading logs directly from FortiGate or analyzing pasted debug outputs. Users can generate complex configurations via natural language prompts, which can be refined in the Code Lab and executed directly. Managed through granular controls, the feature utilizes either FortiAI with monthly FortiCare Premium token allotments (which can be topped up as needed) or personal OpenAI keys via customer billing to streamline workflows and reduce resolution times.
1060700	Introduces GUI-driven FAP packet sniffer setup and PCAP export, eliminating manual CLI and TFTP steps. Provides a more accessible and efficient packet capture workflow.

Feature ID	Description
1119321	Add a new http_authd daemon to perform all administrative authentication, enhancing the efficiency and centralization of authentication processes. Additionally, introduce a new diag http_authd command to monitor session entries, providing improved oversight and management of authentication activities.
1122861	Firmware upgrades for extended FortiGate devices (FortiSwitch, FortiAP, FortiExtender) can now be controlled using several new REST APIs on the FortiGate from a Restful API Client, such as FortiManager. See https://fndn.fortinet.net/ for more details.
1123102	Added support for FortiSASE Sovereign licensing bundles for FortiGate 91G and 901G. With this licensing applied, the GUI and CLI is restricted to read-only after the following CLI settings are configured: `config system sov-sase` `set status enable` `end` After the CLI settings are configured, all FortiGate configuration changes are managed from FortiSASE Sovereign Cloud Orchestrator and Web Portal.
1127168	FortiGate now lets users dismiss specific firmware upgrade prompts for extension devices, reducing unnecessary notifications. Upgrade logs have been improved with distinct IDs to differentiate auto-upgrades from manual ones, and email alerts now include detailed status updates. Additionally, after disabling auto-upgrade and updating, the login GUI prompts users to manually confirm their auto-upgrade preference.
1133400	Optimize memory usage on FortiGate models with 2GB or 4GB of RAM by: • Starting the router daemon only when routing configurations are detected • Reducing the memory reserved for Network Processors (NPs) • Setting nTurbo max frame size to 1500. Interfaces with higher MTU will not offload to nTurbo Affected 2GB model families: 40F, 60F and 50G Affected 4GB model families: 70F, 80F and 70G
1141036	To enhance security and reduce vulnerabilities, FortiGate appliances that are no longer under a valid Firmware & General Updates (FMWR) license or have reached End of Engineering Support (EOES) will now automatically upgrade to the latest patch within their current minor version. This proactive measure ensures that all devices remain protected with the most up-to-date security features.
1141064	A new `config system settings` CLI option `gtp-fgsp-s10-only`, has been added to FortiOS Carrier, enabling the selective synchronization of only S10 GTP tunnels between FGSP peers. This enhancement reduces bandwidth usage and aligns with 3GPP standards, improving FGSP scalability in carrier-grade networks.
1143528	FortiGate now supports a configurable log file-system time-out setting. `config system global` `set log-fsck-timeout <value>` `end`

Feature ID	Description
	When an administrator triggers a file-system check after an unexpected shutdown, the FortiGate will attempt to perform the file-system check during bootup. However, if it is not completed within the timeout, the system will continue booting up. After successfully booting up, the file-system check will occur in the background.
1143535	Adds `proxy-fqdn-host` option to use FortiGuard FQDN in Host headers for proxy connections, making rule management easier on the proxy server.
1154153	A new `disallowed-login-methods` setting has been added to the system admin configuration, allowing administrators to explicitly block specific access methods, such as Console, GUI, SSH, or Telnet, for logging into FortiGate. This feature introduces granular control over login channels, enhancing security by enabling organizations to disable unwanted or less secure access methods.
1158947	Allow manual patch upgrade to work without firmware license. Upgrade to another minor/major version will require a license.
1166853	SCP has been added as a supported protocol for uploading and exporting configuration, firmware, license, and certificate files. This provides customers with a more secure and flexible alternative to FTP and TFTP.
1167560	Introduced SNMP support for five new OIDs to monitor IP pool block size, port range, and client IP range, enabling enhanced visibility into IP pool configurations via SNMP queries.
1176612	A new "Legal Third Party" panel has been added to the FortiOS GUI, providing a searchable and exportable list of all third-party software used in the product, along with their required licenses, license terms, and version information. This enhancement centralizes all third-party licensing details in a single, easily accessible location.
1195216	FortiGate now supports TLS 1.3 hybrid Post-Quantum Cryptography (PQC) key exchanges in SSL deep inspection (flow mode), enabling secure traffic inspection. This enhancement ensures compatibility with modern browsers and PQC-enabled servers that utilize algorithms such as X25519MLKEM768.
1196572	An interface alias can now be displayed in various diagnose and get commands to more easily identify the name of the interface or vpn tunnel. Furthermore the interface alias name is extended from 15 characters to 25 characters.
1202253	FortiGate expands HTTPS management interface capabilities by supporting quantum-resistant TLS algorithms, including hybrid key exchange and PQC certificates. This ensures secure administrative access while maintaining compatibility with non-PQC-capable clients.
1206980	Adds client certificate blocklist enforcement, FortiGate ensures that secure explicit proxy connections are protected against known malicious client certificates listed in the Malicious Certificate Database (MCDB), improving security posture and compliance. `config web-proxy explicit` `  set client-certificate-blocklist {enable | disable}` `end`

Feature ID	Description
1223015	Improves FortiGuard connectivity by expanding default load balancing to five servers and adding flexible GUI controls for serverpreference selection. Users can prioritize public or custom servers and choose multiple override server types, now including the previously CLIonly IoT device collection and Virtual patching query options.
1234219	Support per-VDOM replacement messages and images, enabling administrators to tailor message templates separately for each VDOM and improving control in multi-tenant deployments.
1234531	Enhances FortiGuards rating server selection by removing timezone-based weighting and relying on RTT to ensure connections use the closest, fastest FortiGuard servers. The GUI has evolved from a service-based status to a server-specific display with a new View details button. This provides granular visibility into server IPs, response times, and packet loss, making troubleshooting more efficient.
1250003	Introduces a new default automation stitch (Firmware Upgrade Complete), a new automation trigger (Auto Firmware Upgrade Complete), and a new automation action (Auto Upgrade Complete Email Notification); additionally, the firmwareupgrade email notification has been improved for greater clarity, and the previous default automation stitch (Firmware Upgrade Notification) has been disabled.
1256067	The FortiGate FortiGuard communication protocol (FCPC) is enhanced to accept a new `ForcedUpdate` flag as well as the major.minor.patch-build versioning from the FortiGate. When a FortiGate observes its firmware license is invalid, it will send FortiGuard a firmware upgrade message with the `ForcedUpdate` flag and its versioning. In turn, FortiGuard server will ignore license check for that device and parse its firmware version. If the major and minor version on the upgrade-from and upgrade-to firmware are the same, the upgrade will be allowed. Furthermore logs, notifications and automation stitches are improved to provide clearer indication of auto-upgrade and required-upgrade within its messaging.
1256235	Adds support for preserving permember SNMP system information, including location, description, and contact information. This allows administrators to uniquely identify and manage each HA unit in SNMP monitoring tools, even when members are deployed across different sites.

User & Authentication

See Authentication in the New Features Guide for more information.

Feature ID	Description
1076714	Support SAML authentication in a proxy policy using SCIM. This enhancement extends the existing SCIM client support to authentication scheme using SAML, allowing scim-client to be used as user-database.
1140851	A new GUI-based configuration page for FTM push has been added to complement the existing CLI setup. Previously, users had to manually enter the IPv4 address or domain name of the

Feature ID	Description
	FortiToken Mobile push services server, which required updates when the IP address changed. The new option allows users to select an interface instead. The system will automatically use the current IP address of the selected interface, making it ideal for environments where the WAN IP is dynamically assigned.
1193087	Form based authentication can now enable captcha requirement for submission. Support for: Google reCAPTCHA & Cloudflare Turnstile vendor.
1205792	FortiGate now processes user and group attributes from RADIUS Access-Accept messages for FortiGuest MPSK connections. This enhancement enables dynamic firewall policy assignment for WPA2-Personal and WPA3-SAE SSIDs based on user identity.
1216102	When using SAML authentication in a web proxy, the timeout value of the sign-on URL in the auth query can be configured with the following setting: `config web-proxy global` `  set auth-sign-timeout <30-3600>` `end` This allows the client a longer time to access the sign-on URL to the IdP.

VPN

See IPsec and SSL VPN or Agentless VPN in the New Features Guide for more information.

Feature ID	Description
989101	In this enhancement, TLS 1.3 is added as an option for VPN over TCP. The TLS option can be selected when Allow VPN negotiation over TCP is enabled in the VPN > VPN Tunnels > Settings page. With TLS enabled, IKE and ESP traffic are transported over TLS.
1045092	A new Cloud SDN Orchestration VPN wizard is added to simplify the configurations of a VPN tunnel between a FortiGate and a VPN Gateway or Transit Gateway on AWS. When a FortiGate has an SDN connector established with AWS with the proper permissions, the VPN wizard will create the FortiGate VPN configurations and push the necessary Customer Gateway and VPN tunnel configurations to AWS under the configured VPC. This reduces the chance of mis-configurations and the number of steps to configure a VPN tunnel.
1068354	The VPN wizard for creating remote access and SIA tunnels now defaults to using IPAM for addressing instead of manually entering the client IP range. When IPAM is not enabled, an option is displayed within the wizard to enable it and to assign basic IPAM parameters. Once enabled, administrators only need to select a network size in order to automatically assign a block of address from the IPAM address pool to the VPN clients.
1136844	Re-implement the FEC feature on IPsec tunnel 1. Implement the FEC before encryption, thus FEC traffic can be handled by the NPU. 2. The new design can make the duplicate tunnel and packet feature more easy to merge.

Feature ID	Description
	3. Improve the FEC RS algorithm reed table management to save some resource. **4.** Improve the data and parity packets range and ratio to provide a better recovery effect. The new FEC implementation in 8.0 is not compatible with 7.6 and before, so all devices need be upgraded to 8.0 if FEC is enabled.
1151100	To enhance the resiliency of security posture tag verification before VPN connections, FortiClient endpoints now sends security posture tags in JSON Web Token (JWT) format directly to the FortiGate. This provides a backup mechanism for FortiGate to verify tags when FortiClient EMS is unreachable or slow to respond. FortiGate continues to prioritize querying FortiClient EMS for tag verification as the primary method. This feature requires FortiClient 7.4.5 and FortiClient EMS 7.4.4 or above.
1152420	FortiOS now supports Post-Quantum Cryptography (PQC) for Agentless VPN. This enhancement introduces new CLI options for Agentless VPN, allowing you to select pure and hybrid PQC algorithms to prepare for future quantum computing threats.
1169198	Added support for specifying source geography addresses in firewall policies and policy routes on a FortiGate configured for dial-up IPsec remote access, and matching them based on the public IP geolocation of incoming dial-up IPsec remote users.
1201008	A new per-VDOM setting is introduced to control whether IKE over TCP is enabled for VPN tunnels. `config system settings` `  set ike-tcp-service { enable | disable }` `end` When enabled, dialup VPNs configured in the VDOM will behave as the Auto transport option. Transport over UDP will be preferred, but when the IKE connection cannot be made over UDP, communication will be attempted in TCP. When disabled (default), dialup VPNs will not attempt to connect over TCP. The TCP option for configuring the phase1 transport option for a dynamic-type VPN gateway is therefore removed. Upon upgrade: **1.** If a dynamic-type dialup VPN with auto or TCP transport mode exists, the ike-tcp-service setting is enabled for the VDOM. **2.** If a static VPN with TCP transport mode exists, the ike-tcp-service setting is enabled for the VDOM. **3.** If a static VPN with auto transport mode exists, that VPN will be changed to use transport UDP.
1205594	IPsec VPN over UDP may now use port 443 for the IKE negotiation port. `config system settings` `  set ike-port 443` `end`

Feature ID	Description
1212920	Native VPN remote access configurations have been improved on the VPN wizard. For supported OS's, configurations from the VPN wizard will work out of the box. Native VPN client defaults to using L2TP over IPsec for Windows, Android and macOS/IOS clients. Admins can also configure IKEv2 for Windows and Android clients.
1233077	The ShangMi SM4 encryption algorithm and SM3 hash algorithm have been added as supported proposals for IKEv1 and IKEv2 site-to-site VPN configurations. The SM4-SM3 pair can be selected for Phase1 IKE proposal, and Phase2 ESP tunnel proposal."

WiFi Controller

See Wireless in the New Features Guide for more information.

Feature ID	Description
1078408	FortiAP now supports management over IPv6. This enhancement enables seamless integration into modern, IPv6-based network environments. It improves scalability, simplifies configuration in large deployments, and ensures compliance with evolving regulatory and infrastructure standards
1095618	DARRP channel selection can be handled by FortiAIOps when available, which collects radio data from FortiGate via REST APIs and recommends optimal channels to reduce interference. This shift enables smarter, centralized Wi-Fi tuning in high-density environments like campuses.
1122339	Introducing a configurable option to bypass the default Captive Network Assistant (CNA) behavior on WiFi client devices when connecting to a bridge mode captive portal SSID. When this option is enabled, clients must manually open a full web browser and attempt to access a website to trigger redirection to the captive portal login page. This method improves authentication reliability by avoiding issues sometimes caused by automatic CNA launches. `config wireless-controller vap` `edit <name>` `set captive-network-assistant-bypass {enable | disable}` `next` `end`
1135855	FortiOS WiFi controller now supports dynamic redirect URLs from Cisco ISE. When enabled, clients are redirected to session-specific portal pages without requiring manual URL input, improving integration and user experience.
1139482	Added support for WPA2/WPA3-Enterprise and WPA3-SAE authentication in client mode on FWF G-series models, enabling secure and flexible network authentication.
1144166	The zero-wait DFS functionality, previously exclusive to FAP-U platforms with the default setting as enabled, has now been extended to QCA-based FAP F, G, and K models.

Feature ID	Description
1150610	FortiAPs can now automatically request certificates from EST or SCEP servers configured in the wtp-profile, eliminating the need for manual CA uploads via TFTP. This streamlines 802.1X WAN deployments and simplifies certificate renewal.
1171795	This update enhances the connection stability of FortiAPs to the controller, particularly in cloud environments where network changes can disrupt communication. The system now utilizes a faster and more reliable keep-alive check, incorporating additional session details to facilitate quick reconnection if the data link is disrupted. These changes reduce the chances of dropped sessions and make recovery faster and smoother in dynamic network conditions.
1185065	FortiAP-K models now support Multi-Link Operation (MLO) as part of Wi-Fi 7, enabling simultaneous data transmission across multiple bands (2.4, 5, and 6 GHz) for improved performance and efficiency.
1187056	When customers run an older FortiOS version that does not support a newly released FortiAP model, the AP will now be classified as FAP MVP, a generic Wi-Fi 7 2x2 dual-band profile. This provides limited management and visibility until the user upgrades to a FortiOS release that fully supports the AP mode.
1189365	G/K series FAPs now support up to 16 Virtual Access Points (VAPs) per radio, doubling the previous limit of 8. This enhancement enables more flexible multi-SSID deployments and better service segmentation.
1197458	FortiAPs now support IPSec traffic offload when wtp-profile > dtls-policy is set to ipsec-vpn or ipsec-sn-vpn. A new CLI command allows enabling/disabling this offload, improving client throughput in secure branch deployments.
1208534	Introduces user configurable Clear Channel Assessment (CCA) threshold tuning, giving administrators control over how sensitively a radio responds to channel activity in busy RF conditions. Enhances efficiency and reliability in high density wireless networks.
1210163	A new VAP setting, radius-auth-survivability, allows FortiOS to locally reauthenticate WiFi clients when the RADIUS server becomes unreachable. This keeps previously authenticated stations connected and able to reconnect, reducing service disruptions during RADIUS outages.

ZTNA

See Zero Trust Network Access in the New Features Guide for more information.

Feature ID	Description
1027222	FortiOS 8.0 introduces the ability for a FortiGate to act as a ZTNA service connector to reverse proxy service connections upstream to the ZTNA Edge. In this scenario, the ZTNA Edge may be a FortiPAM or FortiProxy which acts as the ZTNA access proxy to the end users. The FortiGate, as the ZTNA service connector, forms a persistent control connection with ZTNA Edge. The ZTNA Edge forwards connection requests through the control tunnel to the FortiGate ZTNA service connector, which proxies the request to the protected server.

Feature ID	Description
1064352	FortiOS 8.0.0 introduces various configuration simplifications and modularization. Various objects are decoupled so they can be paired together in different combinations within the ZTNA policy. CLI Changes: • firewall.access-proxy configs now split into different objects: • ztna.traffic-forward-proxy • ztna.web-proxy • ztna.web-portal • firewall.proxy-policy now references a new ztna-proxy type referring to the 3 objects above • Introduction of the ztna.destination object for traffic forwarding destinations • ZTNA firewall policy and proxy policy references the ztna.destination object directly for ZTNA traffic forwarding GUI Changes: • Configure ZTNA VIP in the new ports page • Allow ZTNA VIP to be shared by multiple servers • Configure ZTNA web proxy and traffic forwarding on different pages • Support ZTNA Agentless web-portal
1068907	Share used tags that are actively applied in ZTNA policies with FortiClient EMS. `config endpoint-control fctems` `edit <ID>` `set capabilities used-tags` `next` `end` Requires FortiClient EMS 7.4.4 and above.
1145867	This enhancement introduces IPv6 security posture tags and groups which can be applied to dual stack IPv4/IPv6 ZTNA policies. This requires FCT and EMS running 7.4.5 or 8.0.0.

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

FortiGate	Upgrade option	Details
Individual FortiGate devices	Manual update	Use the procedure in this topic. See also Upgrading individual devices in the FortiOS Administration Guide.
	Automatic update based on FortiGuard upgrade path	See Enabling automatic firmware updates in the FortiOS Administration Guide for details
Multiple FortiGate devices in a Fortinet Security Fabric	Manual, immediate or scheduled update based on FortiGuard upgrade path	See Fortinet Security Fabric upgrade on page 55 and Upgrading all devices in the FortiOS Administration Guide.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 8.0.0 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 8.0.0
FortiManager	• 8.0.0
FortiExtender	• 7.4.0 and later
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 and later

FortiAP	• 7.2.2 and later
FortiAP-U	• 6.2.5 and later
FortiAP-W2	• 7.2.2 and later
FortiClient EMS	• 7.0.3 build 0229 and later
FortiClient Microsoft Windows	• 7.0.3 build 0193 and later
FortiClient Mac OS X	• 7.0.3 build 0131 and later
FortiClient Linux	• 7.0.3 build 0137 and later
FortiClient iOS	• 7.0.2 build 0036 and later
FortiClient Android	• 7.0.2 build 0031 and later
FortiSandbox	• 2.3.3 and later for post-transfer scanning • 4.2.0 and later for post-transfer and inline scanning

* If you are using FortiClient only for IPsec VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 8.0.0, use FortiClient 8.0.0.

Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiExtender devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 8.0.0. When Security Fabric is enabled in FortiOS 8.0.0, all FortiGate devices must be running FortiOS 8.0.0.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *Get Checksum Code*.

FortiGate 6000 and 7000 upgrade information

Upgrade FortiGate 6000 firmware from the management board GUI or CLI. Upgrade FortiGate 7000 firmware from the primary FIM GUI or CLI. The FortiGate 6000 management board and FPCs or the FortiGate 7000 FIMs and FPMs all run the same firmware image. Upgrading the firmware copies the firmware image to all components, which then install the new firmware and restart. A FortiGate 6000 or 7000 firmware upgrade can take a few minutes, the amount of time depending on the hardware and software configuration and whether DP or NP7 processor software is also upgraded.

On a standalone FortiGate 6000 or 7000, or an HA cluster with `uninterruptible-upgrade` disabled, the firmware upgrade interrupts traffic because all components upgrade in one step. These firmware upgrades should be done during a quiet time because traffic can be interrupted for a few minutes during the upgrade process.

Fortinet recommends running a graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

Fortinet recommends that you review the services provided by your FortiGate 6000 or 7000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 8.0.0:

1. Use the following command to set the `upgrade-mode` to `uninterruptible` to support HA graceful upgrade:

```
config system ha
    set uninterruptible-upgrade enable
end
```

   When upgrading from FortiOS 7.4.1 to a later version, use the following command to enable uninterruptible upgrade:

```
config system ha
    set upgrade-mode uninterruptible
end
```

2. Download the FortiOS 8.0.0 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
   For example, check the FortiGate dashboard or use the `get system status` command.
5. Check the *Cluster Status* dashboard widget or use the `diagnose sys confsync status` command to confirm that all components are synchronized and operating normally.

Password policy enforcement

After upgrade to FortiOS 7.6.5 or later, the password policy is enforced, and your password must meet the requirements before you can log in to FortiOS. Passwords must contain:

- 1 uppercase letter
- 1 lowercase letter
- 1 special character
- 1 number (0-9)
- A minimum length of 12 characters

If your password meets the requirements, you can log in to FortiOS after upgrade.

If your password does not meet the requirements, you must change your password before you can log in to the GUI or CLI.

Product integration and support

The following table lists FortiOS 8.0.0 product integration and support information:

FortiManager and FortiAnalyzer	See the FortiOS Compatibility Tool for information about FortiOS compatibility with FortiManager and FortiAnalyzer.
Web browsers	• Microsoft Edge 135 • Mozilla Firefox version 138 • Google Chrome version 136 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 135 • Mozilla Firefox version 138 • Google Chrome version 136 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	• 5.0 build 0332 and later (needed for FSSO agent support OU in group filters) • Windows Server 2022 Standard • Windows Server 2022 Datacenter • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Novell eDirectory 8.8
AV Engine	• 8.0014
IPS Engine	• 8.0028

See also:

- Virtualization environments on page 60
- Language support on page 60
- Agentless VPN support on page 61

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.2 Express Edition, CU1
Linux KVM	• Ubuntu 22.04.3 LTS • Red Hat Enterprise Linux release 9.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• Windows Server 2022
Windows Hyper-V Server	• Microsoft Hyper-V Server 2022
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, 8.0, and 9.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

Agentless VPN support

The following table lists the operating systems and web browsers supported by Agentless VPN (formerly SSL VPN web mode).

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 138 Google Chrome version 136
Microsoft Windows 10 (64-bit)	Microsoft Edge 135 Mozilla Firefox version 138 Google Chrome version 136
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 138 Google Chrome version 136
macOS Ventura 13.1	Apple Safari version 18 Mozilla Firefox version 137 Google Chrome version 136
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 8.0.0. To inquire about a particular bug, please contact Customer Service & Support.

Agentless VPN

Bug ID	Description
893190	When using two-factor authentication for SSL VPN users, the FortiGate does not respect the two-factor token timeout configured in config system global. This causes the token to expire prematurely for different two-factor authentication types including email, SMS, FortiToken.
978939	Performance issues occur when CMDB configuration is large.
983513	The two-factor-fac-expiry command is not working as expected for remote RADIUS users with a remote token set in FortiAuthenicator.
1124222	Intermittent connection disruption occurs when using SSL VPN web mode to SSH to Cisco routers with authentication banners.
1164876	Abnormal SSL VPN web portal GUI is displayed when unsupported element is applied in template.
1168008	Security header issues occur when accessing SSL VPN portal
1180110	An error condition occurs during SSLVPN WebMode password renewal
1203158	An error condition occurs when the maximum number of concurrent users is reached
1214345	High memory usage occurs when multiple VDOMs are configured with SSLVPN.
1216477	Blocked IP addresses are cleared when login-block-time is not reached in multiple VDOMs with different login-block-time settings.
1234918	Insecure Content-Security-Policy occurs when SSL VPN portal is accessed
1240901	PCI scan fails when using HTTP/1.0 on the SSLVPN port
1247129	Browser offers to save RDP credentials when Agentless VPN is configured
1257802	RDP disconnections occur when high monitor refresh rate triggers command limit in Agentless VPN web portal
1272207	Authentication failure occurs when username and OTP are concatenated during SSLVPN login on FortiOS 7.4.11

AntiSpam

Bug ID	Description
1228574	Email logs are incomplete when using proxy inspection mode with an email profile.

AntiVirus

Bug ID	Description
1078174	An error condition in scanunit occurs during stress testing
1080003	FortiGate memory is gradually increasing when FortiGate Flow AV Profile is inspecting TCP 6200 traffic with outbreak prevention enabled.
1153880	File upload of a large file fails on an HTTP2 connection when FortiGate AntiVirus is enabled in proxy mode with deep inspection.
1181573	SSL inspection does not correctly add the Authority Key Identifier (AKID) when operating in Flow mode with DPI enabled.
1214247	When FortiSandbox inline scan is configured in proxy inspection mode, timeout occurs prematurely.
1256662	Internal 500 error occurs when AV profile is enabled in the firewall policy after AV engine update

Application Control

Bug ID	Description
673117	Unexpected behavior occurs when FortiGate processes TFTP protocol data under certain conditions.
1118703	Web traffic designated as blocked is allowed due to the config entry priority in the application control profile.
1144469	No security events logged for custom Application Control profiles in Monitor mode when applied to policies configured to log all sessions.
1156066	Communication breaks when application control is used in policy over EMAC VLAN interfaces
1205692	FTP traffic is blocked when Application Control is enabled over Sock5
1217478	Incomplete IEC 60870-5-104 detection occurs when IPS session is cleared.

Bug ID	Description
1260248	Protocol Enforcement fails to block DNS over TCP traffic when non-DNS TCP traffic uses port 53

DNS Filter

Bug ID	Description
1144986	DNS service disruption occurs when FortiGate is deployed as a DNS proxy with DNS filtering enabled and an unreachable SDNS server is preferred.
1150842	Dynamic DNS updates are not forwarded to the DNS server according to transparent-dns-database when using a conditional DNS forwarder for the non-authoritative zone
1151824	DNS query failure when DNS requests received from different VRF with the same transaction ID, source, and destination addresses are treated as retransmissions and discarded
1159583	DNS Filter Rating Servers license not reflected in CLI for 71F when using Single FortiGuard HA license in HA cluster with logical-sn setting
1172192	Server certificate is moved to DNS related configurations when FortiGate acts as a DNS server.
1179030	An error condition in dnsproxy occurs when handling DNS requests for TYPE65 records.
1205688	High CPU usage occurs when a large number of wildcard FQDN objects are configured.
1214420	FortiGate encounters empty-QNAME DNS requests when HA link traffic is misinterpreted as DNS queries.
1222846	FortiGate encounters empty-QNAME DNS requests when HA link traffic is misinterpreted as DNS queries.
1229928	Traffic is not blocked as expected when DNS response returns NXDOMAIN in flow-based mode
1243152	Incorrect client and server cookies are returned for cached DNS entries when conditional forwarding with EDNS cookies is configured
1254463	Traffic drop occurs when using wildcard FQDN objects when a certain pattern of FQDN cannot be resolved by passive learning.
1255195	DNS query failure occurs when FortiGate acts as recursive DNS server for long TXT records

Endpoint Control

Bug ID	Description
1086668	FortiGate does not connect to EMS cloud when EMS cloud license is expired on the global FortiCare account, even when the access keys are valid in other VDOMs
1113593	EMS connector is getting disconnected when using a third-party certificate for verification, resulting in loss of tags and denied traffic.
1129653	An error message appears when endpoint-control override settings are enabled without VDOM enabled.
1207648	Intermittent disconnection of EMS Cloud from FortiGate caused by frequent TPM requests from httpsd
1226271	Memory usage issues caused by EMS endpoint requesting many client avatar entries.
1239851	Traffic bypasses policy when SIA assigned IP is not updated with ZTNA tag

Explicit Proxy

Bug ID	Description
979401	No option to configure IPv6 address pools in explicit proxy policies.
1034891	Web application using SAML IDP authentication in POST method via SWG on FortiGate gets a 303 response and the payload in the post request gets discarded.
1066091	Traffic issue occurs when FortiGate authenticates machine account in the format of HOSTNAME$ using NTLM
1094870	FTPS data connections fail to establish when using flow mode firewall policies configured for FTP service.
1096263	Intermittent 504 errors occur when an IPv6 HTTP request followed an IPv4 request in the same pipeline goes through explicit proxy with outgoing-ip.
1116834	Authentication pop-up does not appear when accessing https websites via FortiGate with Explicit Proxy when authentication Rules, webproxy-forward-server, and certificate-inspection are configured in proxy-policy.
1118847	Explicit proxy policies filtering by HTTP method incorrectly match all traffic, causing unintended deep inspection.
1135770	Group query fails to match for some users after upgrade when using LDAP server authentication with recursive group search enabled in explicit proxy.
1139784	Machine account is treated as NULL user in Kerberos and fails to authenticate via Kerberos.

Bug ID	Description
1149811	An error condition in WAD occurs when auth rules are changed during policy matching in explicit proxy policies
1157551	Memory usage issue caused by improper internal state handling when using WebProxy.
1163040	An error condition in WAD is triggered by an edge case which causes the process to enter an error-handling path
1166344	WAD session freeze when using explicit proxy with HTTP2 enabled in VDOM UKT-Proxy.
1177548	A 400 Bad Request error occurs when accessing CP addresses during SAML authentication in session mode.
1178564	Intermittent policy denied issue occurs when explicit proxy policy is configured with SDWAN zones in outgoing interface
1202441	Captive portal is unavailable when accessing the Internet after firmware upgrade in a situation where a client uses a forward server to access a website
1203767	File upload issues occur when using FortiGate as a proxy with Content-Range header
1209746	Intermittent connectivity issues occur when using FTP Proxy through npu vdom link
1219524	HTTP requests are blocked when request-obs-fold is set to keep and obs-fold is present in Content-Type
1237357	Proxy rule match issues occur when host-regex address values exceed 40 characters
1240208	Intermittent 504 Gateway Timeout errors occur when using explicit proxy after upgrade due to wildcard FQDN not resolving a certain pattern of FQDN
1247518	HTTP 303 Redirect Loop occurs when accessing websites with SWG SSO connection
1252739	Total shared user count exceeds limit when proxy-auth-lifetime is enabled
1253230	Undocumented concurrent explicit proxy users limitats in Max Values table
1257127	Unexpected behavior in explicit proxy occurs when video filter is enabled and there are multiple requests to the same video ID

File Filter

Bug ID	Description
1150204	File attachment names from naver.com are displayed as 'uploadByXHR' instead of their actual filenames
1186664	Outlook web client doesn't update emails automatically when proxy-based file-filter is enabled on proxy policy
1208793	When File Filter is enabled on a proxy policy, some API calls are blocked
1219051	MSI files are not blocked when downloaded in flow mode

Firewall

Bug ID	Description
917883	Virtual server functionality is impacted when using specific cipher suites in FIPS-CC mode
1004263	Session counters are not being updated when ASIC offload is enabled on firewall policy. FortiGate GUI is displaying incorrect information in the "Bytes" and "Last Used" columns.
1057080	On the Firewall Policy page, search results do not display in an expanded format.
1084957	Offloading issues occur when session-denied-offload is enabled for denied multicast sessions
1086315	Some customers observed memory usage increase and client session not disconnecting issues using virtual server
1093616	Bytes counter issue occurs when existing sessions are revalidated on a new firewall policy
1099748	HPE incorrectly identifies TCP RST ACK packets as TCP type when receiving RST ACK packets.
1114635	In the GUI, cannot filter Address objects correctly when using CIDR notation.
1120499	Packet loss occurs when default-qos-type policing is configured on FortiGate-3700F
1134809	Security policy hit counter resets when learning mode is enabled in NGFW policy mode.
1136543	Traffic block occurs when creating 802.1ad type VLAN based on redundant interface
1138259	Traffic carrying VLAN info encounters forwarding mismatch after deleting a VLAN interface built upon an NPU VDOM link
1140803	With interface policy configured with IPS enabled, UDP port 4500 traffic is not offloaded due to incorrect session flag f02 after ICMP unreachable packet is received.
1142813	Filtering by comments fails when quick-editing firewall policies in the Firewall Policy page.
1144475	Intermittent DCE/RPC session blocks occur when two session-sync-dev are connected to the same switch without VLAN separation
1145106	Multicast traffic drops occur when sending large packets to remote tunnels over the x5 interface on FortiGate 400F.
1145129	Port-preserve option changes to disable when disabling NAT in policy
1148161	Erroneous MAC address is used on SOC4 platforms when traffic offloads EMAC-VLAN to VLAN traffic to NPU
1148166	Source port translation was not permitted with traffic to UDP port 7001.
1152839	Asymmetric routing causes ICMPv6 traffic to be blocked by anti-replay when the original direction is offloaded to the NPU while the reply direction cannot be offloaded
1154620	Traffic is blocked by DoS policy when npu offload is disabled under IPsec phase1-interface and DoS policy is configured with parent interface.
1154805	Firewall deny policy mismatch occurs when local user traffic is specified

Bug ID	Description
1155687	DNAT incorrectly in later FTP data packets and FTP data session gets reset when FTP server responds with public IP in PASV mode
1156810	Traffic is logged as accepted in Forward Traffic Log when FortiGate is configured as a DNS server and implicit deny policy is enabled.
1157120	Traffic failure occurs when GRE pass-through has a tunnel key set to zero during offload.
1157283	High priority traffic drops when bursty traffic is present on low priority queues.
1158137	Traffic is blocked when UTM and Nturbo are enabled in firewall policy for np7lite platforms
1158391	Inconsistent address group configuration occurs when using CLI's 'append' command with 'all' value
1159576	Traffic shaping fails when type is set to queuing in the shaping-profile
1160065	Configuration settings in firewall.service.custom altered after upgrading from 7.4.x to versions 7.6.0 through 7.6.4 on FortiGate models with 2 GB of RAM.
1160083	Expected session using its parent session's policy id in the session list is confusing and makes policy match look wrong.
1162875	IPv6 traffic is blocked without sending RST packets when send-deny-packet is enabled for 4.19 kernel
1163826	when non-TCP/UDP traffic passing through the Hyperscale VDOM, the selected SNAT IPPool can be wrong in NAT Source function call.
1164742	SNAT failure occurs when GRE traffic is offloaded on NP7
1169071	Incorrect FQDN translation occurs when passive learning of FQDNs is enabled
1169439	GTP tunnel deletion occurs when mobility handover happens with same PDN connections information
1170304	Websites load slowly when NPU offloading is enabled in firewall policy and the packet length is bigger than the MSS due to many fragmentation needed packets
1171392	No response occurs when FortiGate receives a packet with low TTL and a deny-all policy is set
1176942	Auth-ike-saml-port responds on VIP/IPpool IP address when configured on a FortiGate with mismatched interface IP addresses
1178125	Packet loss occurs when traffic shaping rule is enabled with no limits on per-ip-shaper and the pre-defined max limit is overflow
1178157	IPv6 packets are dropped when block-land-attack is disabled and source and destination addresses are the same.
1178995	Slow upload speed when per-ip shaper is configured with auto-asic offload enabled.
1179233	Geo IPs are only installed into the kernel if the country is used, which makes the option geoip-anycast in firewall policy not work very well

Bug ID	Description
1187335	Video playback issues occur when SNAT is applied and RTSP session helper does not rewrite the destination field
1187861	The diagnose debug flow trace incorrectly displays the operation as DNAT instead of SNAT when a central SNAT policy is matched.
1188448	Traffic drop occurs when configuring virtual wire pair to inspect 802.1Q double tagged VLAN traffic
1188867	An error condition occurs in firewall policies when referencing FSSO usernames with special characters in NGFW policy mode
1189618	Fragmented packets drop when auto-asic-offload and IPS are enabled.
1190878	Incorrect firewall.vip type=server-load-balance global limit in Max Values table
1191592	Traffic is misrouted to the FortiGate login page when a VIP with an unresolved FQDN mapped address is configured.
1194430	WAD logs may display an incorrect destination interface and firewall policy, even though traffic is sent to the correct real server, when a Virtual Server uses multiple real servers in different subnets with separate firewall policies per interface.
1195869	QTM stats issue occurs when traffic is VLAN/IPSEC through hardware switch
1198219	Packets are dropped when using auto-asic-offload with EMAC-VLAN over LACP on FortiGate
1200717	Traffic is allowed by local-in policy 4294967295 when VIP is configured with port-forwarding.
1202418	Incorrect policy matching occurs when multiple DCE-RPC packets arrive simultaneously
1203504	Traffic fails over emac-vlan interface between vdoms when offloading is enabled
1204648	Secondary SCTP session failure occurs when an existing SCTP session has a different source port number than the EXP session
1211358	Service negate enable option is reset to default state when restoring a full-config backup with service-negate enabled in firewall policies
1214413	The handling of "firewall-session-dirty check-all" has been optimized so that changes to interfaces or policies unrelated to the offloaded session will not cause the offloaded session to become dirty.
1215851	Packets are sent back on the same trunk interface when emac-vlan is removed in an emac over LAG setup
1215886	Spoofed reply packets bypass FortiGate when strict check is enabled and reply traffic comes from a different interface.
1216936	NetBIOS broadcast packets are forwarded when netbios-forward is disabled on the same interface
1217157	GeoIP allow/block functionality fails when configuring VIP with GeoIP as source due to a limitation in number of unique countries (256) that can be added to kernel from a firewall policy.
1218523	ICMP packet drops occur when hardware offloading is enabled

Bug ID	Description
1222166	Traffic shaping fails when SD-WAN load balancing is enabled after reboot.
1224865	Passive port translation occurs when FTP helper is enabled despite VIP port forwarding being disabled
1225202	Hairpin traffic is subject to policy check when allow-traffic-redirect and ipv6-allow-traffic-redirect are disabled by default.
1233342	Traffic drop occurs when ipv4-proto-err is enabled on NP7-based FortiGate
1235349	Destination IP addresses become unreachable when auto-asic-offload is enabled on the policy where emac-vlan interfaces are used and VRRP virtual mac is enabled
1238779	Real server URL health check fails when using http-get with http:// scheme after upgrading to 7.4.9
1240706	In NGFW policy-based mode, traffic may be bypassed when the IPS engine is not running such as when FortiGate first boots up, the IPS engine is upgrading or when it is manually stopped with debug commands
1244717	Traffic impact occurs when asic-offload is enabled on NP7 over a one-arm EMAC VLAN interface
1248237	Traffic is blocked when a routing change occurs and a block session exists, even if a valid policy allows the traffic.
1249725	An incorrect IPv6 warning occurs when creating an IP object with ::/128
1252751	Virtual servers with custom SSL ciphers are deleted during upgrade
1257907	NTurbo offload fails when using inter-VDOM links on FortiGate.
1258998	Packets do not match firewall policies when dynamic address contains non-standard dotted IP address after upgrade
1259241	FortiGate forwards packets with incorrect destination MAC addresses when using EMAC interface with VLAN ID
1266899	Traffic disruption occurs when switching NPU's default-qos-type to shaping using QTM module
1267442	ECMP session drops occur when a physical interface goes down
1273283	Session timeouts occur when ECMP routing paths exist and one of the paths is lost.

FortiGate 6000/7000 Platform

Bug ID	Description
881927	An error condition occurs in the system when moving between 3G and 5G with GTP-INSPECTION-GRX profile applied

Bug ID	Description
950983	Feature Visibility options are visible in the GUI on a mgmt-vdom.
1014826	SLBC does not function as expected with IPsec over TCP enabled.
1092619	Session synchronization fails when encryption is enabled on FortiGate models in some cluster setups.
1104967	Intermittent interface disruption occurs after power cycle
1108405	VLAN interface accounting issue occurs when vlif reaches its maximum
1113805	Firewall policy statistics reset after reboot on FGT-6k devices caused by improper persistence of aggregated data.
1117663	Unexpected behavior in the bcm.user process after a factory reset can sometimes prevent the FPMs from booting up.
1135891	The PSU status incorrectly shows as "Critically High" on the GUI dashboard widget.
1136261	Traffic blockage occurs when creating VLAN over redundant interface on SOC5 platform
1146580	Traffic stats aggregation issue occurs when using M ports in FGSP setup
1147340	Duplicated interface entries occur in FortiGate HA configuration merges when the same interface is processed across multiple cycles without successful resolution, causing persistent sync failures and redundant log entries.
1149342	BGP flapping occurs when concurrent IP address management causes unexpected source IP usage on outbound connections during FortiGate VDOM migrations.
1150933	Intermittent packet forwarding issues occur when TCP SYN packets are forwarded between ISF and FPC on FortiGate.
1153360	Counter values fail to match totals and may overflow during continuous clearing in certain FortiGate models.
1154348	CLI allows assigning VLAN interface of M port LAG interface to data VDOMs when configuring VLAN interface on top of M port LAG
1159322	GTP-C tunnel sync issue occurs when using FGSP with load balancing.
1159714	Unexpected behavior observed on certain FortiGate models when configuration changes follow enabling "cfg-save revert" due to unresolved netdevice references in the np7 driver.
1161584	An error condition occurs in the APACER NVME controller during hardware testing on FortiGate-201G.
1166353	VXLAN traffic is removed when offloaded to NP7Lite with VLAN ID.
1170088	RADIUS authentication fails when connecting to Secondary Chassis Slot 2 to 4
1170210	FortiGate Wireless controller Wifi client cannot ping GW/FGT interface. Pass through traffic works fine
1170524	SSH login attempts via special ports fail for VDOM admin users with access to 'mgmt-vdom' on SLBC FortiController models.

Bug ID	Description
1172378	Blades go to dead status when upgrading due to a cross FIM issue.
1172922	SDN dynamic address synchronization flaps or fails when SDN connectors are frequently enabled and disabled.
1173230	Traffic loss occurs when FIM on standby unit is rebooted in HA A-P setup on 7KE model
1173455	Cluster out-of-sync when adding or deleting VDOMs with long names in HA mode.
1173956	Too many addresses included in EMA Tag entry could not be properly inserted as dynamic address objects causing traffic to fail as traffic could not properly match the related firewall policy
1174680	CPU usage issues observed during IPsec tunnel formation over PPPoE interfaces
1178328	Unexpected behavior occurs in the system when IPv6 traffic goes through GRE TP vdom on SOC5 platform
1179530	Create session response is dropped when PGW replies with Context Not Found and TEID is null.
1179961	An error condition in FortiGate occurs when booting up with specific configurations and remaining idle.
1181032	On 6K/7K platforms, confsync out of sync occurs when configuring an ACME certificate.
1182822	FortiGate 320xF and 370xF models may experience traffic drops when NPU is enabled in a firewall policy due to a missing channel.
1183709	FortiGate models fail to install proto=18 routes during initial SD-WAN health check configuration, causing secondaries to miss updated routes unless manually triggered.
1183735	Graceful upgrades lead to unintended primary claiming by FortiGate units during HA resynchronization.
1185009	Traffic on VLAN interfaces is dropped when changing LAG members in emac over VLAN setups due to MAC address changes not being updated.
1185528	Issue description: subscription license on the secondary chassis is missing after the graceful upgrade from 7.2.10 to 7.2.12 workaround: run "execute update-now" again
1185779	CPU usage issues observed during GTP session sync on FGSP nodes
1188338	The MLD state transitions to "Stopped" on the primary FIM when FortiOS incorrectly uses the FPM as the primary instead of the FIM, disrupting multicast6 traffic.
1196215	High CPU usage occurs when session-denied-offload option is missing under config system npu on the NP7 device.
1198697	Link/Activity LEDs remain on when executing shutdown on FortiGate 120G/121G
1203314	FDB sync issue occurs when using NAT vdom virtual-wire-pair

Bug ID	Description
1204630	Traffic disruption when VRF routes are not synchronized to secondary blades.
1211372	An error condition in confsyncd occurs when file sizes change between scans
1211612	An error condition occurs in the ixgbe adapter when using NTurbo with the ixgbe NIC
1214688	Fragmented UDP-ESP packets are not forwarded when received on FortiGate.
1219115	In 6K/7K platforms, SSL VPN load balancing does not work correctly when split-port is set to 1-M1 and 1-M2.
1222830	Management access loss when FIM02 on standby chassis is primary Worker.
1231901	Link-speed test failure occurs when CP10 is configured as Gen4x2
1236300	CPU usage issues observed during BGP downtime and irregular sip traffic is observed
1242828	Erroneous memory allocation may occur under specific conditions on FIMs and the primary FPM during IPv4 and IPv6 routing operations.
1244720	Memory usage issues caused by running v4/v6 routing protocols after upgrade
1253034	VLAN interface counters show zero Receive/Transmit Bytes and Packets when fastpath is disabled
1260299	High CPU utilization occurs when config system npu set lag-out-port-select is enabled
1271514	rsso fgsp sync via traffic port not working #1274662
1272827	Traffic forwarding fails when FGT7081F Primary FPM does not send GARP to connected switch after HA failover.

FortiView

Bug ID	Description
1123502	FortiView Threats: drill down to malicious website entry return Failed to retrieve FortiView data from disk
1138980	Read-only profile admin user try to change fortiview source time range and it logs as edit as system admin in system events
1139219	The Quarantine widget experiences delays when loading the complete IP list.
1141357	Session counts beyond a certain limit are not displayed on FortiView, device icons are missing from FortiView pages, and quarantine actions do not reflect in the Log Viewer.
1146317	Incorrect offload status when NPU Accelerated sessions have an offload value of 9.
1192657	No data is displayed when Cloud is chosen as best available device

GUI

Bug ID	Description
264694	When a firewall user logs in via the GUI using RADIUS with FortiToken, no accounting request is generated.
793029	Unexpected behavior occurs on some FortiGate models when a FortiClient lacks a required MAC address attribute.
853352	When viewing entries in slide-out window of the Policy & Objects > Internet Service Database page, users cannot scroll down to the end if there are over 100K entries.
919473	Network > Interfaces: When there is an IPsec tunnel bound to an interface, "Interface Integrate" for that interface fails
1040164	Interface X1/X2 does not display on the GUI-Network-Interface page faceplate for FortiGate-90G Gen2.
1053139	Login failure messages appear in the GUI when administrators log in within an air-gap environment
1055740	CPU usage issues observed during GUI login with a USB drive containing many files
1063643	GUI interface panel mismatch when FortiGate 121G Gen2 faceplate is changed.
1098643	Unexpected behavior observed in the WebSocket caused by stale connections, resulting in persistent memory allocation errors or Node.js restarts.
1107513	An error condition in Node.js occurs when handling stale websocket connections
1110950	An error condition in httpsd occurs when using JSON array sort compare
1112727	FortiCare/FortiCloud registration is not enforced correctly when accessing FOS GUI, resulting in potential security risks. Registration level is not properly indicated, and admin access is not restricted as expected. This feature is initially supported on the FortiGate 900G series and FortiGate 200G series.
1119321	Authentication enhancements and optimizations using HTTP Admin Auth Daemon
1126162	Hostname pop-up window shows "failed to retrieve info" error in System->HA page
1126975	Timezone offsets are displayed in UTC when a timezone is set
1129254	Unexpected behavior occurs when attempting to save L2TP dialup tunnel configurations using SD-WAN members on some FortiGate models.
1137821	Failed to open CLI console from downstream FortiGate GUI with error "Connection lost." with SAML SSO admin login
1138400	GUI accessibility issues occur when FortiGate is configured with a large number of FAPs and left idle for an extended period
1138545	An error condition in Node.js occurs when writing to a closed client socket
1139922	Cannot rename authorized FortiSwitch

Bug ID	Description
1140317	FAP/FSW registration status appears vacant on Firmware & Registration page.
1141330	Interface bandwidth issues occur when using NP accelerated inter-vdom links
1143611	User/groups objects disappear after editing firewall policy.
1145475	Multicast traffic dropped when add/remove interface bandwidth widget on dashboard
1145510	Unexpected behavior in Node.JS occurs when creating IPsec tunnels through the wizard
1146621	With SSLVPN policy creation for the policies which are created on CLI, when edit the same policy from GUI it is not asking for user/group.
1146967	Failed to update prompt occurs when moving interface using Interface Integrate feature
1148930	Exported FortiSwitch ports to tenant vdom are not displayed on the GUI when the tenant vdom has a fortilink, causing virtual switches to be filtered out due to the lack of a fsw-wan1-peer attribute.
1148959	An error condition in httpsd occurs when fetching data from cmdbsvr fails
1149411	Increased Node.js memory usage occurs caused by errorneous memory allocation observed when Logical and Physical Topology pages are used
1150591	Node.js encounters an error when attempting to read the property from a null value, causing unintended behavior on some FortiGate models.
1152464	The DHCP reservation widget incorrectly validates based on the subnet instead of individual IP addresses.
1152580	FEXT dataplan display issues occur in FortiGate GUI when controlled by FEXT-101G
1152737	When device-identification is enabled, an incorrect IP address is observed when a device gets updated with no IP address
1152849	Connection loss occurs when accessing FortiGate Cloud remote access
1153294	Custom HTML content does not render correctly on login pages when configured through the FortiGate web interface or CLI.
1154487	GUI page times out when never timeout option is enabled for the admin profile.
1156109	Console prints error when logging in to the GUI with dns ssl-certificate set to Fortinet_Factory
1160891	Incorrect inbound traffic values appear on the bandwidth widget for EMAC VLAN interfaces when configured over physical interfaces.
1161725	The new http_authd daemon is added to the Fortinet Security Module FortiSM
1162818	Proxy policy GUI page keeps loading when using user.certificate in ZTNA proxy-policy.
1163464	Read permission occurs when logging in with read-write accprofile if FortiGate is managed by FortiManager
1165258	Address group search results are not returned when there are thousands of firewall addresses and groups.

Bug ID	Description
1165306	FortiSwitches not showing in alphabetical order in GUI occurs when viewing FortiSwitch Ports
1165693	An error condition occurs in the GUI sniffer when using advanced syntax
1166328	An error condition in httpsd occurs when ACME is enabled
1166539	Failed to add Fabric Connector widget in Dashboard when creating serial-VDOM mapping for non-FortiGate devices.
1166936	Failed to load value occurs when viewing PoE devices on FortiOS GUI
1167693	An error condition occurs in the user device store query when accessing the Asset Identification Center page
1169584	An error condition in Apache occurs when the ACME renewal thread interacts with the main thread.
1172647	Filtering services become unavailable when Anycast is enabled
1174970	Configuration changes to FortiGate Cloud SSO Admin settings are lost after reboot
1175204	Incorrect IP address displayed in GUI when fortiguard-anycast-source is set to AWS
1175241	After performing a search in the policy list, sections cannot be collapsed, causing delays in operations
1177282	Failed to save changes when reordering NAC policies via GUI on FortiGate models after upgrade.
1178020	Administrative-access option FMG-Access is not available on the GUI when FIPS-CC mode is enabled
1179698	GUI error when editing the IPsec tunnel when the VPN name contains "/"
1180629	GUI displays username sensitivity warning when username-sensitivity is disabled.
1181363	Failure to load FGD categories when creating or editing webfilter rating override entries.
1182557	VCI options are lost when saving changes on the GUI
1183360	VPN status displays inactive for policy-based VPN
1183906	Incomplete IP list appears when viewing threat feed object entries in GUI
1186022	Filtering issue occurs when Exact Match + Negate columns filter is used for null column value cases
1187233	TAG %%FGT_HOSTNAME%% fails to display in client browser when added to auth-login-page replace message
1189250	Upgrade page display issue occurs when HA cluster is in secondary-only mode
1190608	Permission denied error occurs when Remote+Wildcard administrator attempts to create Web Profile Override in GUI
1191076	Interface bandwidth data is not displayed when LAG is upgraded from 2x40G to 2x100G ports

Bug ID	Description
1191960	Incorrect certificate HASH algorithm name is displayed in FortiGate GUI when viewing certificate information
1192959	An empty page is displayed when clicking FortiTokens in the navigation menu.
1193206	Faceplate fails to load after editing an interface
1193884	Vlan interface bandwidth displays incorrectly in GUI dashboard widget when LAG members are removed and re-added.
1195382	In Edit FortiAP dialog, Transmit power mode cannot be overridden when 8 SSIDs selected on wtp-profile.
1196284	SecurityFabric tooltip displays Client IP when device is detected as a router
1196746	GUI displays 'Invalid address group selected' in IPsec when 'Interface Subnet' type is selected for IPv4 split tunnel address
1197356	Search function issues occur in Asset Identity Center when searching by device name or OS
1198106	Inaccurate SD-WAN spillover algorithm description when priority values are the same.
1198508	Incomplete filter options occur when navigating to the Policy & Objects > Firewall Policy page
1198609	Memory usage issues caused by Node.js forking when using the JIT optimizer in V8.
1199029	DHCP Server conflicts occur when changing from DHCP Server to Relay mode on an interface
1200410	Incorrect power supply status appears when the power cord is connected to the right PSU only under WiFi and Switch Controller.
1203007	Configuration view issue when logging in with FortiGate Cloud SSO super_admin account.
1203716	Memory usage issues caused by Node.js compressing or decompressing in a thread are resolved by forking a new process.
1203957	Inconsistent license expiration dates appear when viewing license information
1205624	Warning message displays when creating Phase 2 in IPsec without matching encryptionauthentication pairs to Phase 1 proposal.
1206994	Memory usage issues caused by Node.js data compression and decompression
1208267	GUI displays a blank page after logging in as a vdom-admin with 2FA.
1209188	Warning message occurs when checking asset details page and switching to disk log
1211830	Cannot login to GUI sometimes after vdom-admin timeout
1212726	Authentication issues occur when using FortiCloud SSO via FortiGateCloud login
1214354	When Security Rating runs a full report on devices that have hundreds of extension devices, device becomes unresponsive when node process CPU and memory utilization suddenly increase
1214424	Authentication failure occurs when logging in to the GUI after upgrading when post-login banner is enabled

Bug ID	Description
1215061	Memory usage issues caused by Node.js writing to a closed socket
1215246	Interface deletion fails via GUI on hardware-switch but succeeds on CLI
1216367	Access issues occur when admin with custom accprofile logs in to GUI
1217015	Faceplate loading issue occurs when hovering over WAN interface in multi-vdom mode
1217386	Incorrect label appended in comment after copying and pasting policy on GUI
1217474	Unexpected behavior in Node.JS occurs when executing workerpool scripts
1217546	Login failure occurs when using 2FA admin through GUI in edge case due to FortiSM policy violation
1219066	NAT is enabled automatically when toggling security posture tag in ZTNA policy
1220268	Less prominent warning for NAC VLAN Segment occurs when switch does not support it
1220854	Read-write mode is displayed after login with read-only vdom-admin when FortiGate is managed by FortiManager.
1221215	Slow GUI performance occurs when searching address groups
1223774	Firewall policy GUI page shows 'no-inspection' for SSL when profile group is applied.
1224951	Interface aliases do not display in Performance SLA columns when configured in FortiGate GUI
1228240	An error condition occurs in the GUI when editing Block/Allow lists under Email Filter
1230037	Changes occur when FortiGate is managed by FortiManager and admin logs in with read-only access.
1233052	An error condition in Node.JS occurs when token generation fails.
1234222	An error occurs when switching the table from Performance SLAs to SD-WAN Rule
1234864	Error condition occurs when checking SIM status Carrier on GUI
1235147	Virtual server clone function becomes edit mode when clicked
1236970	FortiSM Violation is observed when revision backup on logout is enabled and super_amdin logs out from the GUI
1237463	Login failure occurs when post-login-banner is enabled with SAML Single Sign-On
1239075	Policy dialog page fails to update source object when changing from internet-service to regular address during policy editing
1239337	User passwords cannot be printed in clear text when logged on with guest admin account
1239562	GUI access fails when a custom GUI certificate is configured that uses SCEP enrollment and a certificate renewal occurs during a HA switchover
1242637	Firewall policy search issues occur when searching for External Feed objects in a long list
1245838	Incorrect mode option appears for WWAN interface when LTE modem is enabled

Bug ID	Description
1247676	SSH deep scan toggle does not save when enabled on low-end models.
1249169	Incorrect Japanese translation occurs when prompted for one-time upgrade when critical vulnerability detected
1249302	An error condition in Node.JS occurs when handling undefined properties.
1249390	Detailed asset vulnerability info fails to display when accessing the Asset Identity Center page or Asset FortiClient widget
1251014	Incorrect interface stats occur when master FIM miscalculates bandwidth and throughput on SLBC platforms
1256988	Brute-force attacks triggered a lot of leaving http_authd processes running and causing memory usage to steadily increase.
1258180	Display limit in source and destination columns of policy list is increased from 3 to 5 when FortiGate is configured.
1265195	GUI performance issue occurs when adding or removing members from large firewall address groups

HA

Bug ID	Description
984306	Session synchronization fails when encryption is enabled in FGSP with IPsec VPN setup.
1017177	A WAD processing issue causes the SNMP to not respond in an HAcluster.
1075828	Firewall unresponsiveness occurs when HA failover happens with high resource utilization
1080655	HA synchronization fails after configuration changes on FortiGate devices due to improper handling of a hasync flag in the fgfmd daemon.
1096472	Traffic disruption occurs when moving VDOMs between VClusters
1121141	IP address is not released by DHCP client when MAC changes during HA enablement
1126274	VDOM is created unexpectly when changing VRRP priorities on multiple interfaces if standalone-config-sync is enabled
1129731	Intermittent session disruption occurs when rebooting the standby firewall
1133589	HA cluster fails to form when FIPS-CC is enabled
1142218	Source IP cannot be selected when HA-direct is enabled and multiple ha-mgmt-interfaces are configured.
1143361	Downtime occurs when upgrading HA cluster with HA encryption or authentication enabled due to HA communication being sent through IKE tunnel when tunnel is not ready

Bug ID	Description
1143791	The heartbeat interface default route is lost and HA fail to sync when changing the interface mtu-override option
1148845	LDAP authentication fails when ha-direct is enabled due to confusing logic between which interface takes priority when interface-selection is also used
1148862	HA synchronization issues occur when user local password expiration and UUIDs are mismatched
1151668	B2731:Interface bandwidth widget does't display HB and Managed port
1154466	Traffic forwarding issues occur when FGSP failover happens
1160030	CPU usage issues observed during ICMP error packet processing in FGSP clusters
1160292	FFDB version sync issue occurs when updating on-demand ffdb in HA environment
1162432	Split brain occurs when renaming IPsec phase1-interface in a HA cluster with a lot of VDOMs.
1163147	Token license activation fails when using a virtual serial number (vSN) on a new HA FortiGate
1165361	CPU usage issues observed during HA led optimization with child process forking
1165798	An error condition in FortiMQ occurs when HA AA is configured and malware-stream scan is enabled on primary FortiGate.
1168328	Mgmt interface is lost when joining a device to a cluster with system dedicated-mgmt enabled.
1170763	Device synchronization issues occur when removing a device from FortiManager
1170958	HA status shows as 'Unknown' when changing HA group ID
1171987	HA not synced after modifying onetime schedule when cfg-save is manual
1172590	An error condition occurs in FortiGate when running the "diag sys ha nonhaconf" command on the secondary node in an HA cluster
1176985	Traffic drop occurs when UTM is enabled on firewall policy with FGSP configured
1178208	VLAN HB link monitor stops working when HA Group-ID is set above 255
1179351	FortiGate failed to load the private keys for factory certificates to fgfmd due to incorrect classification
1179821	Intermittent connectivity loss occurs to HA secondary management IP after upgrade to v7.4.8
1180636	Session filter issues occur when adding custom service filters with different port ranges under cluster-peer session sync.
1184781	Intermittent HA sync disruption occurs when changing tunnel interface IP address on FortiGateVM in Google cloud
1187401	Unexpected behavior in the system occurs when an HA unit is restarted
1190477	An error condition occurs when creating vdom-exception for system.central-management on HA-enabled FortiGate-VM.

Bug ID	Description
1191128	Intermittent traffic disruption occurs when the secondary FortiGate is rebooting in HA mode.
1191136	HA ports cannot be added to an aggregate interface on 340xE & 360xE
1193802	FortiGate 120G/121G Link and Activity LEDs do not turn off even after "execute shutdown"
1203672	Config overwrite issue occurs when restoring config from TFTP server on master via CLI in HA setup
1206861	CPU usage issues observed during hasync usage of the sslvpn reserved UDP port 8903
1207127	Backup failure occurs when executing backup config via reserved management interface in multi-Vdom
1207182	An error condition occurs when hasync or fgfmd retrieves the config
1208912	Session loss when AS path prepend redirection is used after rebooting an FGSP peer.
1209223	Traffic will fail when setting up a new cluster and immediately pinging from the secondary unit to outside
1212718	FGFM tunnel remains down after HA failover event when undestroyed fgfm session prevents new fgfm sessions from being created.
1213917	Interface configuration deletion occurs when QOS is enabled and a reboot happens
1214587	DNS queries are sent from HA reserved management interface when it is configured.
1216459	Verification failure occurs when BIOS security level is set to High during HA image upgrade
1217228	Route table deletion occurs when a split brain condition happens in GCP
1220647	RX drops occur on HA1 and HA2 ports when upgrading the i40e driver
1221816	Network instability when FIM is rebooted on primary after failover using 'diag sys ha reset-uptime'.
1223506	Traffic forwarding issues occur when FGSP asymmetric traffic and layer2 are enabled with the first member's id set to 0
1223805	IP address remains when interface with BFD enabled is removed from HA cluster
1224802	HA out-of-sync occurs when 'set cfg-save manual'
1224835	Traffic drop occurs when doing HA failover on EMAC VLAN
1225710	Mobile Token assignment fails on old models that don't support vSN when HA fail-over occurs
1225919	Packet size issues occur when syncing large FQDN response packets in autoscaling environments
1226672	Packet loss occurs when slave member emac-vlan responds to ARP requests in an HA setup with LACP and VLAN.
1226946	High CPU usage occurs in HA Sync process when receiving incomplete scripts.

Bug ID	Description
1231480	LACPDU transmission issues occur when HA failover is triggered by a monitoring port disconnect
1234340	Asymmetric session handling fails when two FGSP links are configured and only the second link recovers after both go down.
1235313	Traffic disruption occurs when a large number of firewall policies are installed after a failover during an upgrade in a FortiGate cluster
1235326	HA synchronization delay occurs when using a custom acc-profile
1237317	No Rx packets occur when unicast-hb is enabled on FortiGate-VM64 with SRIOV.
1240288	Packets are sent using the cluster MAC address by the secondary cluster member after failover
1240503	Realserver status remains up when previous primary becomes secondary after HA failover
1241700	When a backup unit in an HA setup is rebooted and rejoins the cluster, traffic to a downstream host connected to the LAN hardware switch is interrupted for ~15 to 20 seconds due to STP
1243380	Virtual MAC is used by HA-AP Secondary when removing a member from an aggregate interface
1244401	Virtual cluster member dead logs occur when non-primary blades in chassis report HA related logs
1244800	An error condition in Confsync occurs when sending large messages through the local socket
1246577	IPAM is unexpectedly enabled on the HA peer when CSF is enabled or modified.
1248579	Traffic disruption occurs on EMAC VLAN interfaces during HA failovers
1250174	Autoscale synchronization issues occur when configuring FortiToken on system admin
1250511	Unexpected Layer 2 bouncing occurs when dev_base is missing
1268268	DHCP server offers use physical MAC instead of VMAC when HA is formed after reboot or upgrade
1271901	Authentication issues occur when Azure SDN connectors reuse incorrect tenant tokens after HA failover
1273912	Split-Brain state occurs when configuring a new VDOM when the primary has more VDOM license seats than the secondary unit
1274545	Both nodes respond to ARP requests when the HA table is edited in config sys ha.
1275737	License Status: Warning occurs when root VDOM is active on the primary in a FortiGate-VM HA A/P cluster with VDOMs and virtual clustering enabled.

HyperScale

Bug ID	Description
1089281	with FG480xF/FFW480xF using npu-group other than "0" with log2host with around ~1M CPS could result in NP chip getting stuck
1138921	Suggest to change the default NPU setting to reduce the high-frequent of spv/tpv table messages
1143144	Both HW log(ps) rate and log(pm) rate showing in dia sys npu-session stat when set log-mode per-nat-mapping
1150073	For previous versions of hyperscale FortiOS, FGCP HA clustering with hardware session synchronization with config vcluster-status disabled allowed you to monitor hw-session-sync-dev interfaces. FortiOS 7.6.3 changed this behavior and you can no longer monitor hw-session-sync-dev interfaces. When upgrading to FortiOS 7.6.3 if your HA configuration includes monitoring hw-session-sync-dev interfaces, the upgrade will fail. You can work around this problem by removing monitoring from hw-session-sync-dev interfaces or by selecting different interfaces to be hw-session-sync-dev interfaces before performing the upgrade.
1150863	Unintended session deletion may occur after FGSP failover due to a dirty Rsession.
1155548	With host logging (log2host) enabled, session counts may begin to rise after a few days of operation. This rise in session count can reduce throughput and CPS performance. You can work around this issue by restarting the FortiGate.
1159964	Incorrect duration of hardware sessions occurs when the system is up for a long time
1184045	IPv6 TCP/UDP traffic fails to pass through when a threat feed object is integrated into an IPv6 High Security policy due to an internal state handling issue, which erroneously disables IPv6 functionality.
1199557	Unsupported network interfaces are permitted as members of a Link Aggregation Group (LAG) when the LAG is configured for hardware session synchronization, leading to potential configuration errors.
1204615	Improvements to session management to resolve memory usage issues when creating hardware sessions.
1212583	Add the CLI implemented in br_7-0_np7_cgn_dse_timer_refresh to the GA trunk
1223847	Excessive hyperscale logs occur when log-mode is set to per-mapping
1245165	ICMPv6 type 2 packets are dropped when SIP ALG and Hyperscale are activated

ICAP

Bug ID	Description
1028368	ICAP connection queue full errors occur when the max connection count is split and allocated to each worker.
1220371	Empty page occurs when using ICAP profile with $Domain in header after successful authentication

IPsec VPN

Bug ID	Description
842821	Accounting information is not sent to RADIUS when EAP and 2FA authentication are enabled
1045098	IPv6 traffic is blocked on new configured IPsec VPN over loopback interface, need reboot to fix it
1048998	IPsec tunnel RX & TX counters discrepancy occurs when SDWAN health check or local traffic is sent through the IPsec tunnel
1063528	Incorrect MTU settings prevent fragmented packets from being properly offloaded in IPsec tunnels, causing high CPU usage on FortiGate models.
1063737	High CPU usage occurs when using IPsec tunnel with fragmented packets and UDP frame size of 1600B.
1068626	SOC4 platform IPSec traffic may stop in specific corner cases due to the IPSec outbound process becoming unresponsive.
1101897	Abnormal spikes in VPN traffic sent bytes occur when counters roll back due to race conditions.
1104203	TX counts are doubled for local traffic sent through IPsec tunnels on NP7.
1106454	IKE debug prints large number of "compute DH shared secret request pending" when rekeying or DH group setting not matched on both sides.
1107163	After upgrade, the default DH group in IPsec is set to 20 or 21 instead of 14, 20 or 21 causing connection failures
1112964	IPsec VPN connection issue occurs when interface 'a' is used in the policy instead of the ipsecvpn interface.
1127782	Traffic is dropped by anti-spoof check when passing traffic through phase2 transport mode with GRE encap.
1128662	BGP peering fails to establish when a race condition occurs between FortiGate OS and NPU driver during IPsec SA updates for dynamic hub-to-static spoke VPNs.

Bug ID	Description
1131498	Deletion of tunnel interface fails when linked to another IPsec tunnel interface
1133207	Tunnel establishment fails for multiple FortiGate clients when using DHCP-over-IPSec dial-up VPNs during high concurrent connection attempts.
1137576	IPSEC tunnel failure occurs when IKE Diffie-Hellman processing fails
1140823	IPsec tunnels become stuck on spoke np6xlite, causing ESP packet drops after extended operation due to improper vifid formation during multiple rekey operations.
1141865	Decrypt counters do not update when SA is offloaded
1142334	BGP failure occurs when VPN interface name is changed
1144548	Authentication failure occurs when using IPsec VPN IKEv2 with MsCHAPv2 and radius server
1145391	IPsec VPN tunnel fails to establish when QKD is required due to failure to complete SSL handshake with the QKD server
1146975	IPSEC tunnel issues occur when NPU offload is enabled on SOC4 platforms and a very large packet arrived without fragmentation
1147023	VPN traffic halts unexpectedly on the spoke when FEC is disabled during connection cleanup after failed phase 1 negotiations, affecting dynamic tunnel handling.
1149340	Fragmented packets are not sent out on vpn-id-ipip IPSEC tunnel when npu-offloading is enabled
1152486	Unable to select policy-based ipsec tunnel in the firewall policy for SD-WAN member while configuring in GUI.
1153363	Intermittent disruption occurs on ipv6 route lookup when configuring IPsec with FIPS-CC enabled
1153984	Authentication error occurs when IPSEC-IKEv2 tunnel is configured with FortiToken Cloud
1156722	DNS suffix search issues occur when using IKEv2 phase1 dialup gateways with mode-cfg enabled
1158032	Incorrect source IP used for IKE packets when multiple prefixes are configured using SLAAC
1162270	Secondary IPsec tunnel cannot come up after primary tunnel is down and config change when "set monitor" is configured under phase1
1162563	An error condition in the system occurs when creating more than 75 VPN tunnels with Egress Traffic shaping enabled
1162740	Multicast traffic above 1350 bytes does not flow through the IPsec aggregate tunnel when using pre-encapsulation.
1164175	DH group mismatches with INVALID_KE when peer proposes a DH group in its IKE_SA_INIT which is not in the expected order
1167952	Packets with payload larger than 10K and smaller than 15K are dropped when using IPSec tunnel as egress interface with nTurbo enabled

Bug ID	Description
1168556	IPv6 routing entries remain after iked restarts
1169860	L2TP connections fail when L2TPD experiences internal errors while attempting to create tunnels for clients.
1170094	An error condition in IKE occurs when using TCP transport
1172040	Returning packets take a different path when TCP transport is used with multiple default routes in the routing table.
1173228	During modeconfig setup, an IPSec IKEv2 dialup tunnel may install a default route when no IP address can be allocated from the pool.
1174914	IPsec tunnel sourcing from secondary IP address instead of primary IP occurs when local-gw is set and then unset on the phase1-interface
1177724	RADIUS Framed-IP-Address assignment issue occurs when using IPsec IKEv2 and 2FA
1179347	Intermittent IPSec tunnel disruption occurs when upgrading to FortiOS 7.4.8 with FIPS enabled in HA mode
1179794	VPN IPSEC client to site connection fails when EAP proxy times out.
1180324	Auth-ike-saml-port setting is lost when set to 10443 during FortiGate update or reboot
1180987	VPN tunnels may not come up after HA failover events, causing routes via these VPN tunnels to not be added to the routing table.
1181552	An error condition in IKE occurs when using TCP
1181945	Traffic disruption occurs when using IPv4 IPsec with loopback interface in TCP transport mode
1182043	When 'local-gw' is changed to 0.0.0.0 under the dial-up IPsec VPN interface and DHCP servers failed to respond to DHCP discovery but FortiGate kept previous IP in kernel, errors are displayed in the debug logs
1182937	Unnecessary RFC6311 recovery occurs on primary tunnel when receiving IKE SA sync from other FGSP members
1184605	Firewall policy issues occur when a new policy is created for a connected VPN user without explicit mention in the policy.
1186237	Under high traffic and session load, CPU utilization increases when a remote access VPN user connects or disconnects
1190688	High CPU usage occurs when changing firewall policies in a FortiGate device with a large number of policies.
1192598	IPsec phase1-interface option 'loopback-asymroute' is not available for IKEv1
1195129	Intermittent traffic disruption caused by error condition in IKE daemon when connecting to Dialup IPsec IKEv2 on Azure VM64
1195400	Reauthentication failure occurs when using IPsec IKEv1 after upgrade

Bug ID	Description
1195785	High CPU utilization occurs when IKE handles async DH errors during IKEv1 phase1 or phase2 rekey
1197607	An error condition in Iked occurs when using FortiClient to dialup IPsec with SAML authentication on Azure FGT-VM.
1199265	Intermittent traffic disruption occurs when IPsec tunnels are stuck and the engine hangs on the SOC4 platform
1199815	Intermittent IPsec traffic disruption occurs when IKE tunnel status is out of sync with kernel
1200084	IPsec tunnel dec/enc counters fail to update when NPU offloading is enabled
1200669	VPN setting is deleted after device reboot when password policy is enabled and pre-shared key length meets minimum requirements
1200709	Intermittent BGP disruption caused by DPDK enablement
1201212	Reply traffic is dropped when anti-spoof check fails
1203271	DPD probes are sent excessively when dpd-retrycount is set to 0
1204679	Radius authentication issues occur when packet fragmentation happens over IPsec tunnels
1205816	Certificate validation fails during EAP when changing authentication method from signature to PSK via GUI
1206506	Traffic disruption occurs when IPsec tunnel manager write sequence issue happens
1209759	IKEv2 connection fails with "gw validation failed" error when the peer's ASN1DN ID contains multiple OU fields
1210730	Drv-drift counter increase occurs when sending TCP traffic through IPsec with vpn-id-ipip encapsulation
1213238	Authentication issues occur when syncing FortiIdentity Cloud users through LDAP for IPsec IKEv2 tunnel with EAP-TTLS
1214434	Signature verification fails due to issues with the SCEP re-enrollment procudure
1215724	IPsec tunnel establishment fails when FIPS-CC mode is enabled and DH group 31 or 32 is used.
1217216	DHCP requests fail when FortiGate sends the full DN instead of the CN in Option 61 during IKEv2
1217988	ADVPN Dynamic BGP remains active after IPSEC disconnection when Bring Down -> Entire Tunnel is used on the parent tunnel.
1218530	Error condition occurs when using Duo Proxy LDAP application with MFA
1218538	Traffic drop occurs when tunnel ID changes from random 10.0.0.x to remote gateway public IP
1219594	Connection reset occurs when using the same TCP port for IPsec SAML and IKE TCP encapsulation on PPPoE interfaces
1223316	Incorrect local ID is sent during IPsec phase 1 when localid-type is set to address

Bug ID	Description
1227222	IKEv1 transport mode issue occurs when FortiGate is behind a NAT device
1229448	IKEv2 peer selection fails when using AES256GCM-PRFSHAxxx encryption proposal.
1232771	IKEv2 phase1 policy fails to honor interface association when using IPv6 Link Local or duplicated IPv4 addresses.
1238778	Decrypt counters fail to update when NPU offload is enabled
1242217	When ike-tcp-port is set to 443, a VIP created on the IPsec underlay interface can still be connected
1245740	MTU reduction occurs when using IPsec with GCM on 9xG and 12xG devices
1246635	IPsec tunnel disruption occurs when Phase-2 rekey completes with incorrect CHILD-SA deletion.
1248524	File download fails when FortiGate encounters IPSec VPN with set encapsulation vpn-id-ipip and AV proxy and NAT-T
1249753	Old assigned IP address remains in routing table when tunnel is flushed or renegotiated on client side with mode-cfg enabled.
1252546	Negotiation timeout occurs when entering OTP within 120 seconds validity period
1252712	Static route removal issues occur when IPsec VPN is down
1257646	High CPU usage occurs when using IPsec over TCP and receiving an RST packet
1262715	Intermittent VPN disconnections occur due to an error condition in IKE on a Hub gateway
1264833	SAML IPSEC VPN connection fails when connected to a WiFi network via Tunnel SSID

Intrusion Prevention

Bug ID	Description
899659	Inaccurate session anomaly frequency values appear when threshold is exceeded under full-offload conditions.
983372	An error condition in IPS engine occurs when accessing safebrowsing.google.com
1077638	In NGFW Policy Mode, FortiGate may incorrectly block packets from established TCP sessions if no matching IPS session exists.
1091118	Oversized packets exceeding the MTU cause delayed ACKs, leading to unintended behavior
1093769	Unexpected IPS UTM logs may be generated in NGFW policy mode for unknown applications.
1107273	New packets on established SCTP sessions are dropped during processing after a four-way handshake when UTM is enabled.

Bug ID	Description
1110788	Memory usage issues caused by configuration changes or rule loading
1117043	Fatal errors occur when the IPS engine sends requests with zero-length data segments to IPSA.
1122188	Internal diagnostic commands fail or delay when ipsmonitor processes each request sequentially due to sequential forwarding to IPS daemon processes.
1129130	Intermittent traffic disruption occurs when FortiGate is in NGFW mode and it encounters traffic which are legitimate but do not create a session
1131911	Memory usage issue observed in IPSEngine 7.00560 during high SMTP traffic due to improper memory management.
1140846	Unexpected behavior observed in the IPSEngine when handling HTTPS traffic using HTTP/2 in certain configurations.
1144684	High CPU usage occurs when processing multiple RTSP streams due to inefficient resource management by the RTSP decoder.
1152040	An error condition occurs in custom IPS signature when using --log after upgrade to 7.4.5
1152384	CPU usage issues observed during intense IPS packet scanning
1156180	Unexpected behavior observed in the IPSEngine caused by an invalid numeric entity.
1156490	When inspection mode is proxy, inspect-all is enabled and http-policy-redirect is enabled, traffic is not sent to WAD for processing and consequently dropped
1157185	High CPU usage occurs in IPSEngine when traffic looping happens due to incorrect VRF validation in local-out path.
1157469	Disabling nTurbo acceleration causes traffic outage for existing sessions due to sessions not being marked as dirty
1158024	Packet drops and lower CPU utilization on FPC blades when using IPv6 traffic with np-accel-mode enabled and auto-asic-offload.
1158524	Unexpected behavior observed in the IPSEngine when a DNS packet matches a policy with DNSFilter and Safe Search enabled.
1159041	SSL errors occur when accessing certain websites via IPv6 in FortiGate flow mode with SSL inspection enabled.
1162794	Unintended behavior occurs in the IPS Engine caused by the SCADA dissector.
1167574	An error condition in Ipsengine occurs when root Fortinet Factory key and certificate do not match
1168037	Error condition occurs in proxy mode when using inspect-all certificate-inspection in ssl-ssh-profile
1182461	High memory usage occurs when multiple HTTP2 connections with many open streams are present.
1190395	Intermittent traffic disruption occurs due to an error condition in the IPS Engine caused by a DAC handler issue.

Bug ID	Description
1191598	High CPU usage occurs when HTTP2 connections have a large number of open streams
1193876	Memory usage issues caused by improper closure of HTTP2 streams
1197659	An error condition in IPS engine occurs when processing HTTP traffic
1199243	Definition file update issues occur when device-identification is enabled for a zone interface in the firewall policy.
1208885	DSCP 7 marking is not applied when Windows Update traffic is not application-identified in a VDOM.
1210836	Conserve mode occurs when IPSEngine memory usage increases due to gradual increase in AnonPages.
1211362	Decrypted traffic mirror MAC address changes do not take effect until IPS Engine is restarted when used in a firewall policy
1212296	Package download failure occurs when IPS profile is enabled
1216974	Intermittent traffic disruption caused by an error condition in the IPS Engine during hybrid key generation.
1218520	BFD flaps occur due to an error condition in the IPS engine caused by QUIC traffic.
1225743	An error condition in IPS Engine occurs when executing ssl_add_defer_log during stress testing
1239080	Abnormal traffic log behavior occurs when FortiGate is running in sniffer mode with ips-sniffer-mode enabled.
1249177	High CPU usage occurs when IPSEngine scans SMB traffic
1252636	An error condition in IPS Engine occurs when upgrading to v7.6.6
1253472	Unexpected behavior observed in the IPS Engine during HTTP header processing involving buffer edit cases on FortiGate models.
1259235	An error condition in ipsengine occurs during upgrade to 7.4.11
1269354	An error condition in IPS engine occurs when handling unusual TLS 1.3 stacks.

Log and Report

Bug ID	Description
611460	On FortiOS, the Log & Report > Forward Traffic page does not completely load the entire log when the log exceeds 200MB.
1087235	Only last 24 hours of Forward traffic log are been downloaded while trying to download logs from the last 7 days
1087534	Page loading issues occur when loading a high number of logs

Bug ID	Description
1094030	URL truncation occurs in logs due to mismatched length limits between FortiOS and IPSEngine.
1100945	The "Resolve Unknown Applications" feature in the GUI Log Viewer is not functioning as intended.
1113588	FortiGate prompts error "Fetching data from Disk is taking longer than expected. Suggest trying a different log source or check the availability of Disk." when viewing logs for the last 7 days from disk or FortiAnalyzer
1116246	An error condition in locallogd occurs when the system enters memory conserve mode
1119074	An error condition in Syslog occurs when processing misaligned incoming cmdb messages
1127636	Unnecessary log generated when disabling an interface.
1128940	Security Rating summary log displays incorrect counts when triggering a security rating check
1129247	Certificate verification fails when using OFTP custom certificate with non-Fortinet organization name.
1139748	Different logs appear when unplugging PS1 and PS2 on FortiGate.
1141733	Traffic interruptions occur when revisiting the forward traffic log page during searches with applied filters.
1142836	Broadcast traffic is no longer logged when local-in-deny-broadcast setting is disabled.
1143662	Username is truncated in application logs when it exceeds 31 characters
1146443	Inaccurate Netflow reports occur when ICMP long live sessions exceed the active timeout value.
1148101	Logs fail to appear in FortiAnalyzer, and FortiView sources are missing from the Dashboard.
1151300	Logs are not displayed in FortiGate CLI when using free-style filter with timestamp and FortiAnalyzer as data source.
1154982	CPU usage issues observed during high syslogd activity
1162518	FortiGate loses connectivity with FortiAnalyzer when changing interface-select-method to SD-WAN and DNS fails to resolve the address.
1168738	Syslog packets are not sent when log server IP is not configured.
1170889	Traffic log issues occur when updating specific APDB versions
1171020	Authentication logs are missing when 2FA timeout occurs during SSLVPN authentication
1175276	Syslog-override setting status reverts to disabled when restoring VDOM configuration with syslog-override enabled
1177974	Audit logs are not received by FortiAnalyzer when FortiAnalyzer is enabled or disabled in FortiGate.
1180038	Time zone information is missing when set to GMT
1180182	Alert email fails when device is rebooted under HA mode

Bug ID	Description
1184366	Incorrect logs are displayed when applying a destination filter in Log Viewer for remote log sources FortiAnalyzer and FGT-cloud until a hard refresh is performed
1185876	Log daemon resolves server IP reliably when using dnsproxy daemon
1189755	When user performs a log search and also triggers a drill down for more logs simultaneously, the page may be stuck in loading.
1190659	Log search issues occur when searching for a specific mac address in the GUI.
1193296	IPS log display issue occurs when double quote is in agent field
1193350	GTP logs are not visible when log-imsi-prefix is set to a non-numeric value
1197727	Incorrect CEF format occurs when forwarding logs with FTNTFGTaction field
1198455	An error condition occurs when running ITS test
1200810	CPU usage issues observed during quarantine logging
1205249	An error condition in fgtlogd occurs when the device query feature is enabled
1210810	System log issues occur when exiting memory conservation mode
1212825	Frequent SSL VPN statistics event logs are generated when numerous users connect.
1222874	Incorrect deny log occurs when anti-replay is set to strict and Challenge ACK packet is allowed
1223900	Execution log failure occurs when sending test-connectivity from SSH
1226196	HTTP transaction log displays IP instead of URL when client disconnects before server response forwarding
1229712	Failed to get FAZ's status occurs when changing static route settings
1232929	Warning about FortiAnalyzer connection remains on report page when navigating back from Log settings page
1236184	An error condition in locallogd occurs when disk space is full on FortiGate.
1236902	Traffic logs display service group names instead of individual services when service groups are used in firewall policies after upgrading from 7.2.11 to 7.4.9
1239708	Logs are not written to the disk queue when the memory queue reaches its limit.
1240481	IPS log-packet files are not cleaned up when retention time exceeds maximum-log-age
1241191	FortiGate resolves FortiProxy as a PC Hostname when device type is Router
1244679	When configuring syslog over TLS with mutual authentication, FortiGate allows invalid certificates to be configured by allowing certificates without the "client auth" ExtendedKeyUsage
1249376	Unknown app and appcat fields occur when updating APDB from built-in version to 35.00157
1253334	Intermittent disconnection occurs when FortiGate connects to FortiAnalyzer
1272019	An error condition occurs in the GeoIP database during updates

Proxy

Bug ID	Description
764143	SSL version restrictions not enforced in flow mode when using 'min-allowed-ssl-version'.
776013	CPU usage issues observed during HTTP2 usage
859182	WAD encounters an error condition when configuration changes affect certificate verification processes with Crypto KXP enabled.
1107594	Slow website loading occurs when using certificate inspection with proxy inspection-mode in HA Active-Active mode.
1124557	An error condition occurs in WAD when wad-restart-mode is set to time and wad-restart-start-time / wad-restart-end-time are configured.
1133100	Memory usage issues caused by WAD leaking SMB2 session objects when clients close connections with a Kerberos status of KRB_AP_ERR_MODIFIED
1146601	With proxy inline-ips, WAD daemon gets memory leak and leading to conserve mode
1155170	Memory usage increases unexpectedly during high load when processing WAD-related tasks.
1155858	RD Gateway fails behind HTTPS Virtual Server when using WebSocket upgrade
1159485	Traffic duplication may occur on FortiGate due to retransmission of out-of-sync TCP streams when insecure ciphers are used.
1159963	Expired server certificates are issued when Deep Inspection is enabled due to improper handling of certificate cache renewals.
1161940	An error condition in proxyd occurs when migrating from 500E to 901G.
1169917	Websites may fail to load when inspectall certificate inspection and application control are enabled in proxy mode after upgrading to a build that supports Encrypted ClientHello (ECH)
1171499	Certificate chain is not sent during SSL inspection after upgrade.
1173291	Memory usage issues caused by missing certificate memory free operations during stress testing.
1177929	Memory usage issues occur in WAD when handling a large number of sessions
1178184	SSL errors occur when accessing a specific website due to an unexpected record type when Web Filtering and DPI are enabled in Flow mode.
1180097	An error condition in WAD occurs when using HTTP2 or HTTP3 with concurrent authentication requests
1183893	Handshake failure occurs when using explicit web proxy with deep inspection to access HTTPS websites through HTTP requests.
1189141	An error condition in WAD occurs when handling large query responses.
1190329	Memory usage issues caused by insufficient resources during application processing

Bug ID	Description
1191144	An error condition in WAD occurs when sec-default-action is set to accept under web-proxy explicit
1197212	WAD incorrectly prioritizes the default FortiGuard CA bundle over user-installed CAs when building certificate chains for cross-signed server certificates.
1213247	504 Gateway Timeout shown when a virtual-server configured in full mode connects to a HTTPS server that only supports TLS <= 1.2 and which also only supports using SHA1 for signatures
1213957	TCP download rate drops when FortiGate uses SSL inspection with an antivirus profile in flow mode.
1220714	On 200G series FortiGate, some private keys are not loaded resulting in HTTPS traffic description caused by the missing private keys
1224915	Intermittent page could not be reached issue occurs when authentication is required by QUIC
1228854	HTTP status code 302 is not forwarded to the client when ssl-http-location-conversion is enabled
1233324	High memory usage occurs when inline IPS is enabled with long-lived connections and IPS DB updates.
1247379	CPU usage issues observed during large HTTPS downloads
1250721	SMB traffic fails when routed through two VDOMs with IPS/AV enabled with proxy mode.
1255610	TLS active probe failure occurs when proxy inspection is enabled
1266880	Certificate error occurs when connecting to https://x.x.x.x with an ephemeral certificate having DNS Name: x.x.x.x in SAN

REST API

Bug ID	Description
993345	The router API does not include all ECMP routes for SD-WAN included in the get router info routing-table command.
1154124	Adding dynamic fabric addresses via the FortiNAC REST API fails due to an issue with HTTP header validation.
1174023	Invalid values in 'name' and 'group' fields occur when using GET /api/v2/monitor/webfilter/fortiguard-categories
1175330	Incorrect FortiGate configuration returned when long-vdom-name is enabled
1186413	Incorrect POE max value is returned when querying REST API for FortiGate 400 series switches
1196325	API requests fail on HA secondary FortiGate via HA management port when API user has VDOM scope.

Routing

Bug ID	Description
1005523	Deletion of manually added IPv6 neighbor records fails when in NUD_PERMANENT state
1036123	BFD for BGP takes interface BFD config instead of multi-hop config when BFD is enabled on both OSPF and BGP
1097855	IPv6 traffic may be sent to the wrong destination interface or route, causing connectivity issues.
1112999	High CPU utilization occurs when multicast traffic is forwarded across VXLAN from spoke to spoke
1142290	An error message appears in FortiGate when attempting to add the ssl.root interface to a route-map via the GUI
1142955	High CPU usage occurs when link monitor daemon fetches session counts on every interface during REST API calls.
1149245	BGP peering resets occur when changing BGP neighbor configurations in a confederation-enabled environment
1150878	The IPoE tunnel interface cannot be selected in the Interface Bandwidth widget.
1151626	Auto-completion issue occurs when typing IPv6 BGP neighbor commands
1151848	IPv6 BGP flap occurs when FortiGate FGSP cluster connects to Dell Sonic
1152976	Spokes using remote-as-filter with 4-byte ASN cannot establish BGP neighborship
1156431	PIM error when receiving PIM Assert with SSM enabled during HA failover
1157835	Private AS removal issue occurs when remove-private-as is enabled in a neighbor-group and local-as is private
1158738	BGP AS path prepending character limit issue resolved by increasing the set-aspath character limit in route-map
1162962	BGP service disruption occurs when the LAG interface flaps
1164316	IPv6 route issues occur when set delegated-prefix-route enable
1165424	The behaviour of the command `diagnose ip router bgp <module> <enable | disable>` is incorrect. Turning on debugging for one of the modules turns on debugging for all modules
1166008	VRRP version 2 failure occurs when adv-interval is configured in milliseconds
1169479	The SLAAC IPv6 address does not get flushed after link goes down.
1171689	Incorrect route selection occurs during BGP redistribution with route maps due to improper handling of parent protocol distances.
1175185	LSP packet drop occurs when FortiGate sends LSP data in multiple packets without authentication header in subsequent packets

Bug ID	Description
1188061	Incorrect BGP4-MIB bgpLocalAS OID value occurs when 4-byte BGP AS is configured higher than 2147483647
1193345	Warning message occurs when PIM-DM interface root is loopback
1193788	BGP TCP Auth Options key-chain is not applied to the BGP neighbor, causing the neighborship to not establish.
1195004	Conditional-advertise6 fails when using prefix-list6 with action deny and le 128.
1195531	Incorrect route tag occurs when redistributing OSPF routes into BGP
1196770	BGP default route installation issue occurs when capability-default-originate is enabled
1197960	BGP peer flaps when stressful traffic is present on the interface with Quality of Service enabled and top priority
1200779	BGP peering issues occur when using a Class E router ID
1202262	PIM failure occurs when using virtual-switch interface
1204553	OSPF multicast packet transmission failure occurs when changing OSPF interface settings
1217353	BFD session failure occurs when using a loopback interface as a BGP neighbor
1220090	IPv6 aggregate configuration occurs only in VRF 0 when configuring BGP aggregate-address6
1226758	Routing issues occur when HA flaps and monitored interfaces go down simultaneously.
1230742	VXLAN connectivity issues occur when configured with inter-VDOM IPsec underlay between two FortiGates.
1231287	BFD session disruption occurs when remote discriminator mismatch is detected.
1237854	Traffic drop occurs when BGP NEXT_HOP attribute for VPNv4 routes is not updated.
1243609	Route flapping occurs when external routes are redistributed into BGP
1244747	Traffic disruption occurs when using ISCSI boot volume after a reboot
1246350	Traffic does not honor vrf-select when using loopback interface IP as source-ip
1246749	Traffic drop occurs when Verizon Dynamic Network Mobility Routing is configured with a GRE tunnel
1247150	BGP session ends when interface is down in non-zero VRF after hold down timer expires
1247172	BGP sessions remain down when using VRF option due to invalid BGP Identifier
1251244	OSPFv6 neighborship failure occurs when FortiGate is upgraded to FortiOS 7.6.5
1269208	BGP routes disappear from the FIB when pre-encapsulation is enabled on VPN Phase1.
1270500	VRRP info for IPv6 is not returned when running SNMP queries for IPv6 configurations.
1272774	Policy route update issues occur when VPN interface names are changed

SD-WAN

Bug ID	Description
1051429	Dynamic BGP session remains on initial shortcut even when out of SLA.
1138635	Speed-test failure occurs when using ECMP routing configuration from Hub to Spoke.
1142171	Health check status change behavior occurs when recovery time is set to 240 and interval is set to 500ms
1147720	Traffic forwards to the unexpected egress interface when duplicate SD-WAN rules exist in the proute list in the case that priority-zone in sdwan service has only one sdwan member
1147727	Encapsulated traffic of GRE tunnel interface over VNE tunnel egressed wrong interface after reboot
1153432	Downtime occurs when using OSPF with LAN during shortcut establishment and tunnel failover
1153992	Event log used wrong reason that packetloss over the threshold when SLA fails due to consecutive probes failed
1155927	SD-WAN Service events are not logged in SD-WAN Events when using SD-WAN rules in standalone mode
1157493	SDWAN rule with multiple mac address entries only uses the first mac address when address type is mac.
1159877	Hash-mode remains visible when SD-WAN service mode is changed to priority
1160832	Loss of internet access occurs when SDWAN member's gateway overlaps with ippool's IP range
1164937	Incorrect outbandwidth calculation occurs when IPsec tunnel interfaces are used in SDWAN configuration.
1167276	All participants of SLA name become unavailable when the check interval is set to 15 seconds
1176538	Traffic between spokes occurs when shortcut is out of SLA or dead with load balancing enabled and fib-best-match tie-break.
1179004	Speed test failures occur when running multiple tests concurrently on BGP over loopback designs
1181497	Incorrect data type occurs when using OID fgVWLHealthCheckLinkBandwidthBi
1187007	GUI issues occur when accessing SDWAN rules and Performance SLA menus
1190583	SDWAN health check status inconsistency occurs when using manual mode with IPv4 and IPv6.
1192488	Link Monitor failure occurs when HTTP response header has an invalid format.
1199707	SIP traffic issue occurs when TCP syn-ack packets use a different egress interface than the syn packets.
1203173	SD-WAN member fails to return to active state after PPPoE interface instability

Bug ID	Description
1203917	SD-WAN interface status becomes Unknown when Health Check SLA is good
1220599	Traffic matches SD-WAN rule when empty address-group is used as source address
1234194	Non-participant members appear in latency and packet loss columns when viewing the performance SLA page
1239537	Speedtest failure occurs when total latency exceeds 800ms between HUB and Spoke.
1254899	Unhealthy out-of-SLA BGP community is sent unexpectedly after HA switchover when all members are in-sla

Security Fabric

Bug ID	Description
1006397	In case of failure during a federated upgrade process, the system does not report granular failure details for individual devices.
1071882	High CPU usage may be observed in Node.js in environments with many extension devices (FortiAP, FortiSwitch, or FortiExtender), which can cause GUI instability.
1076439	Security fabric Asset Identity Center shows "Failed to load user device store data"
1085248	FortiGate encounters CPU and memory usage issue when loading 20 large external threat feeds (100K entries each)
1110643	Security Fabric issues occur when running FortiOS 7.4 or 7.6 with 200G
1118086	An error condition occurs when enabling CSF root on 50G series devices
1149817	Security Fabric > Physical Topology: Fortilink Tier2 switch shows directly connected to FortiGate on Security Fabric - Physical Topology page. The correct topology can be seen on the WiFi & Switch COntroller > Managed FortiSwitches > Topology view.
1150382	Security profile names containing two forward slashes (//) cause the webpage to become unresponsive when attempting to edit
1156006	SFTP backup fails when triggered through automation stitch on a FortiGate in an HA cluster using Windows-style paths.
1165624	Topology page load failure occurs when CSF is disabled
1166189	When using the OCI SDN connector, dynamic IP addresses are not fetched correctly if the target compartment contains more than 100 VNICs.
1180555	Threat feed connections fail during SSL handshakes when server-identity-check is enabled for HTTPS downloads in FortiOS.

Bug ID	Description
1191533	FortiAP upgrades/downgrades fail to complete properly after an HA failover using "diag sys ha reset-uptime" in a FortiGate CSF topology.
1191902	Automation stitch sync issue occurs when HA secondary unit is used in Security Fabric.
1210303	APIC device overload occurs when FortiGate logs in multiple times without proper logout.
1217270	Automation action-type cli-script fails to execute when triggered by admin login event logs
1224923	IP collection fails when Azure returns a SubscriptionNotFound 404 error
1225433	Automation Stitch variable truncation occurs when using json-c version 0.18 with webhook actions
1228317	Local-in policy creation issue occurs when Security fabric is enabled on non-NPU VDOM links
1239953	Automation stitches fail to execute when FortiAnalyzer sends a security-event notification
1254426	Email notification failure occurs when HA failover happens in downstream FortiGate

Switch Controller

Bug ID	Description
873384	MAC move issues caused by no support for mac move feature on the switch-controller.
947247	Wired clients are not displayed in physical topology when connected to FortiSwitch.
961142	An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver.
1075365	Upgrade or restart of FortiSwitch fails when FortiLink is in HTTPS mode
1105000	Aggregate FortiLink went down, need to manually down/up the interface.
1114032	The GUI becomes slow or unresponsive when transceiver-related API requests fail.
1134306	VLAN configuration mismatch occurs when configuring LAN Extension and VLANs locally on FEX
1135460	Health status becomes unknown after renaming a switch in the switch controller on some FortiGate models.
1137075	In the WiFi & Switch Controller > Managed FortiSwitches page, the Topology view shows the link between FortiSwitch units with a dotted line instead of a solid line.
1137213	Extension device registration fails through GUI when FortiCare agreement acknowledgment flag is reset after updates.
1138263	FortiSwitch port configurations fail to update and GUI display issues occur when user-info process overloads system resources with excessive connections.

Bug ID	Description
1138430	Increase managed-switch.switch-id to more than 16 characters
1141909	The 10G port on FortiGate-120G is not coming up when connected to a FortiSwitch S148F port using a 10G DAC cable
1144076	High CPU usage occurs in cmdbsvr when FortiLink is enabled and FortiLink interfaces are connected to the firewall.
1149256	Renamed FortiSwitch failed to sync to secondary FortiGate
1153868	Sync errors occur when renaming a FortiLink switch with special characters.
1154530	When renaming the switch name in FortiGate with 36 characters, the last character is missing after being pushed to FortiSwitch
1155546	Duplicate entries occur in the switch-controller managed-switch list when renaming a managed-switch.
1164685	Local MAC addresses are filtered out from being added to user device list when mab-entry-as dynamic mode is enabled on Fortiswitch
1165703	Random devices not matching to NAC policy occurs when multiple MACs are present on the same user-device-store entry
1170323	Interfaces cannot be enabled as FortiLink interfaces on FortiGate with hardware revision 2.
1174647	Fortilink connections may not display correctly in the FortiGate GUI Topology view when using MCLAG aggregation
1183135	Filtering by allowed VLANs fails to display expected results when using certain FOS versions
1195908	Virtual VLAN switch forwarding issues occur when STP is enabled in HA setups with multiple members on FortiGate-600F.
1198110	FortiSwitch disconnection observed when adding managed-switch.
1208846	Authentication issues occur when upgrading FortiGate due to Radius auth type mismatch
1216623	High CPU usage occurs when Fortilink IoT triggers packet capture in switch
1216633	Unable to change switch name when space is in the name.
1220590	Intermittent connectivity loss occurs in FortiSwitches when upgrading FortiGate to v7.6.4
1229555	Incorrect VLAN assignment occurs when NAC policies use hostname filters with NetBIOS Name Service group names.
1231001	PoE control issues occur when NAC mode is used on FortiSwitch ports.
1232304	FortiSwitches go offline when upgrading FortiGate from 7.2.10 to 7.4.x
1236067	Devices connected to FortiSwitch remain online when unplugged and idle for more than 30 seconds.
1238312	VLANs from other VDOMs are not added to the port when allowed-vlans-all is enabled.

Bug ID	Description
1239300	Incorrect port information is displayed when running diag switch-controller switch-info port-stats command
1239751	FortiSwitches go offline when upgrading FortiGate from 7.2.10 to 7.4.x
1244391	Empty PORTID occurs when FortiGate switch-controller is connected to FortiSwitch stacking setup
1249140	Blank output occurs when running diagnose switch-controller switch-info mclag peer-consistency-check
1249243	Ports fail to work when configured with the same settings as other working ports after VLAN reconfiguration in a FortiGate HA A-P cluster.
1254816	Authentication fails when both hardware and software switches have 802.1x security mode enabled with mac-auth-only

System

Bug ID	Description
828849	No "Diagnostics" information is available for Avago AFBR-79EBPZ Bidi transceivers on FortiGate when using the get system interface transceiver command.
900936	The fnbamd service may terminate unexpectedly due to erroneous memory handling during certificate authentication, if DNS responses include both IPv4 and IPv6 addresses and one (e.g., IPv6) is unreachable.
906269	An error condition occurs in EXT4-fs when booting without a backup image installed
908309	LLDP packets not received on management interface when LLDP is enabled on certain FortiGate models.
918574	Unintended traffic sent to public servers occurs when cloud-communication and include-default-servers settings are disabled on FortiGate models.
945871	D-NAT functionality fails when using a Software Switch in explicit mode due to incorrect session matching during packet forwarding.
978171	Performance issue occurs when high rate of NP7 DSW drops and ReasmFails happen
986926	FGT-90xG ULL interface x5, x6, x7, x8 are all down after set to 25G speed
991285	Broadcasts are unexpectedly forwarded between VXLAN peers when certain FortiGate models are configured as hubs in a Hub-Spoke topology.
992323	Traffic interrupt when traffic shaping is enabled on 9xG and 12xG
996863	Automatic firmware update email alerts triggered after each reboot on FortiGate.
1015698	FGT601F X5 to X8 interface with 25G SFP28 DAC was down after upgrade to 7.4.4 or later

Bug ID	Description
1024737	On FortiGate, when set ull-port-mode is set to 25G, ports x5-x8 show a status of DOWN.
1039956	FortiGate 601F port x6 keeps flapping after upgrade
1042577	FortiGate does not detect transceivers and interface X8 not coming up after upgrade
1044794	After installing a .deb image during bootup device shows "File - 1 seems to be corrupted" error and cannot boot up.
1046484	After shutting down a SOC4 FortiGate (FGT-40F/FGT-61F/FGT-81F/FGT-100F) using the "execute shutdown" command, the system automatically boots up again.
1048684	The FortiGate Internet Service Database (ISDB) update mechanism fails on a 100E FortiGate model due to insufficient memory allocation.
1057094	Disabling GRE auto-asic-offload on a FortiGate model causes traffic to be dropped due to unrecognized GRE tunnels, likely because the kernel fails to process them without proper configuration post-disabling.
1058256	Some FortiGate models experience unexpected interface down time when using DAC cables after upgrade, due to improper Signal-OK loss detection.
1061796	Inaccurate traffic counters display for EMAC-VLAN interfaces when VLAN ID is set to 0 and traffic is offloaded to the NPU.
1065869	SCTP CRC check option is not available on NP7lite platform like 91G/121G.
1070603	Traffic drop occurs when bandwidth exceeds certain thresholds on NP7lite platform
1071229	Ping reply packets are dropped after two successful requests when using VXLAN over IPsec on FortiGate.
1075340	Aggregate link down occurs when speed is set to 10000auto after upgrade to v7.4.5
1075607	Traffic interrupt when traffic shaping is enabled on 9xG and 12xG
1082891	FortiGate reboot immediately after changing ull-port-mode to 25G without a confirmation prompt.
1083626	FortiGate 90G/91G auto-negotiate support for shared SFP ports.
1095801	Error "Fail to del default npu-vlink setup" is shown when changing the hostname.
1096384	Warn user when restoring config from a different firmware version
1096537	High CPU usage occurs when making configuration changes with a large number of policies.
1099770	NP7 drops encrypted GRE packets that have Checksum bit set (1) due to invalid checksum
1102417	Huawei LTE modem E3372 not recognized on FGT-90G
1107270	Communication over VXLAN are lost after upgrade on NP7 platform
1113064	Memory usage issues caused by running simulator stress test on FortiGate
1113651	An error condition occurs in the simulator during stress testing

Bug ID	Description
1114298	FortiGate Cloud remote login triggers 2 admin login events (1 successful and 1 unsuccessful for PKI admin)
1117005	CPU spikes and management access issues occur on certain FortiGate models post-upgrade when IPsec Phase 1 NPU-offload is enabled during maintenance.
1121078	TX Power levels are missing when using FTL4E1QE1CFTN QSFP+ER transceivers on FortiGate devices.
1121522	Memory leak in slab causes the system to enter memory conserve mode. The issue occurs due to out-of-order log packets and incomplete session scrubbing, resulting in residual entries in the log2host table.
1122446	GPS location updates fail to occur when the GPS signal reception is poor on FortiGate devices.
1124535	DNS Search list options are appended to Router Advertisements when using IPv6 prefix delegation with SLAAC
1131516	CRC error count reset issue occurs when using the diag netlink interface clear command.
1135440	Unexpected behavior occurs when changing interface mode or static route through an IPSEC-Tunnel when emac vlan interface based on npu-vlink is used
1135974	FortiGate-50G-5G fails to get an IPv6 address when set pdp-type ipv4v6
1137218	VXLAN traffic uses primary IP address instead of secondary IP address when configured vxlan remote-ip with secondary IP
1138155	DNS(TCP853) fails until idle timeout when link monitor failover occurs in dual internet connection
1141832	Interface inbound/outbound information is not displayed on the bandwidth widget and CLI when using VLAN interfaces with NP6 platform.
1141907	Unexpected behavior occurs when deleting IPv6 reflect session
1142785	False SNMP alerts occur when a non-installed power supply unit is detected
1142805	Cannot set source IP for FortiGuard when a non-root vdom is set.
1145397	When editing user exemption configurations via the GUI on FortiGate devices, unexpected behavior occurs due to a mismatch between GUI and CLI data structures.
1146354	The network interface settings page fails to load on certain FortiGate models when the admin profile does not have the System > Configuration > Read/Write permission.
1148843	Unstable LTE 4G connection occurs when using IPv6
1149006	DHCP lease delivery issues occur when auto-discovery-receiver is enabled and IPsec tunnels are flapping
1149202	ICOND application startup issue occurs when using raw type over IPSEC tunnel on FortiGate Rugged 70F
1149508	WAN interface goes down when share-port medium type changes to 'copper' after upgrading FortiGate-80F-DSL

Bug ID	Description
1149814	An error condition in WAD occurs when executing log messages with invalid node pointers.
1151313	gtp tunnel list counters don't increase when restore configuration file with "gtp-enhanced-mode enable" on NP7 models
1152059	Device information is not detected when device-detection is enabled in ARM based models
1152638	FortiGate still sends reset packet when drops TCP SYN packets with ident-accept enable on wwan interface after reboot
1152792	Unexpected behavior in the system occurs when installing new objects from FortiManager
1153004	APN profile not updating when configuring Verizon APN
1153276	FortiGate with NP7 processors terminating VXLAN-over-IPsec connections may notice traffic drops during broadcast storms
1153442	Concurrent sessions drop significantly when low-end FortiGate models have low free memory.
1153983	Registration status remains unknown when re-adding FortiManager IP after it was lost.
1154158	DHCP issue occurs when configuring hardware switch interface in A-P HA mode
1154920	Intermittent 10G SFP+ link establishment issues occur when FortiGate-200F reboots and connects to a Ciena 3924 switch
1155410	High memory consumption occurs when Node.js encounters catastrophic failures and creates excessive logs.
1155432	An error condition occurs in cid-scan when the invariant about reference count for a cid_host and the cid_host zombie list is broken
1156561	NP7lite platforms might encounter high softirq issue and stop processing traffic after one month running
1156785	Device recognition issues occur when device-detection is enabled for some Apple devices
1157402	Modem disconnects occur when using Verizon SIM with a strong signal
1157490	Temperature is out of range with unreasonably high value.
1158451	The keytab setting with config user krb-keytab is not changed after toggling private data encryption
1158452	Traffic disruption occurs when creating EMAC-VLAN interfaces with traffic running in the background
1158975	FortiGate does not establish VNE tunnel caused by a failure to commit DNS servers to the CMDB after receiving a DHCPv6 information request.
1159425	Unused power supply log appears in diagnose alertconsole list when a redundant power supply is not used
1159561	Deletion of vdom-link interfaces fails when created using simultaneous SSH sessions
1160215	An error condition occurs in snmpd on FortiGate-VM64-AZURE approximately every 1.5 hours.

Bug ID	Description
1160683	Windows Wi-Fi clients unable to obtain DHCP IP due to dropped fragmented CAPWAP packets on virtual switch interface.
1162489	The SFP WAN1 and WAN2 ports on the FGT-80F device remain down after a reboot when the speed is set to 100M.
1162853	IP lease issues occur when using BOOTP protocol without record
1163292	VDOM expansion issues occur when upgrading license on FortiGate-201G.
1163814	Memory usage issues occur when newcli processes are not deleted after their parent sshd process died.
1164174	Configuration loss on FGT-60F when FortiGate enters extreme conserve mode
1164761	SFP+ direct attach cables are shown as "compliance is unspecified" by the "get system interface transceiver" command.
1164836	NTP server unable to be set with 64 digit key in FIPS-CC mode
1165059	Unexpected behavior in system occurs when executing factory reset on FortiGate-70F
1165172	CPU usage issues caused by receipt of packets longer than 65535 octets
1165701	NP7 HTX drop UDP packets with incorrect checksum.
1165706	SSH and Web CLI sessions are disconnected when generating a TAC Report.
1166455	TCP packet drop occurs when sending traffic over VLAN+redundant port
1167234	Unexpected behavior occurs when loading build B3553 on FortiGate-101F
1167271	Link LEDs on FortiGate 401F are lit when no cables are attached.
1167426	High CPU usage occurs in the linkmtd daemon when large traffic is present.
1168062	Config overwrite issue occurs when importing FortiGate YAML config using the current Python library
1168786	100G ports turn up after reboot when administratively down on platforms with Marvell switch like FortiGate 480xF.
1168792	Network detection issues occur when the LED is on during diagnose hardware tests.
1169167	VDOM link interfaces are not visible when single-vdom-npuvlink is enabled on non-NP7 platforms
1169448	iPad device name appears as MAC address in logs and DHCP Monitor when connected via WIFI to FortiGate
1170291	WWAN interface fails to get IP address when 'auto-connect' feature is enabled.
1170335	Incorrect Option 67 value returned when client sends DHCP INFORM packet with matching Option 60 value
1170464	Memory usage issues caused by low memory availability on FortiGate-51G

Bug ID	Description
1170716	Failed attachment to tower occurs when using custom APN with FortiGate 50G-5G modem
1170933	MTU inconsistency occurs when creating a new LACP interface without a member interface and then adding a member interface later.
1172295	FortiGate does not autoupdate router objects in full such as key-chain, route-map, and prefix list, causing FortiManager to purge the config during installation.
1173177	High CPU usage occurs when making a configuration change on FortiGate-6301F devices, causing CPU Core0 to spike on all FPC and MBD.
1175134	Message server status goes down when configured with loopback as source
1175384	"Partition ImageEXT4-fs (sda2): couldn't mount as ext3 due to feature incompatibilities" when running "diagnose sys flash list"
1177037	System events are not generated when FortiGate acts as a DHCP client
1177302	Output truncation occurs when running the diagnose ips memory status command
1178017	10G Copper interface fails to come up when directly connected after a fresh setup
1178199	SNMPD access issues occur when increasing VM memory
1178202	VLAN tag is stripped when forwarding VXLAN packets between spokes.
1178583	DHCP relay strips DHCP END Option (255) when relaying DHCP packets.
1180084	ZTP deployments fail on FortiGate 9xG Gen2 devices because DHCP client mode is not configured by default on interfaces a and b.
1180734	After a FortiGate upgraded from 7.4.7 to 7.4.8, an unexpected behavior occurred.
1181444	USB-Tethering fails to work on FortiGate 91G when configuring it as a WWAN connection.
1183678	QSFP-28-CWDM4 transceivers in ports 33 and 34 of FortiGate 2600F show as down after upgrading to 7.6.3
1184180	Unexpected behavior occurs when restoring an invalid configuration with a system.interface defined as type aggregate and a system.virtual-switch with the same name.
1184749	PPPoE connection failure occurs when Multilink MRRU is enabled on a VLAN interface
1185286	An error condition in Newcli occurs when executing the get system fortiguard-service status command
1187981	DDOS policy not properly installed in kernel on FortiGate 120G and 121G.
1188182	DHCP server failure to deliver IP addresses occurs when auto-discovery-receiver is enabled and IPsec tunnels are flapping.
1188339	STP forwarding fails after rebooting when stpforward is enabled on a hard-switch interface.
1188905	Unresponsiveness occurs when MTU calculation is incorrect in function np_fragment
1189192	An error condition in cid-scan occurs when processing packets after scanning disablement

Bug ID	Description
1189896	Link failure occurs when using 3M DAC cables between FG90G and FS148F
1190267	An error condition in search_core_tag occurs when rebooting FortiGate-3960E with B3589
1191813	Connectivity issues occur when auto negotiation is enabled on the Cisco switch end
1191833	Inaccurate LAN and WAN speed values occur when running the hardware NIC-led test.
1192249	An error condition in dhcp6s occurs when running on G models
1192440	SNMP sensors report down when snmpd rebuilds interface cache
1192920	Packet capture hitting buffer limits when capturing a high volume of matched packets
1193889	Certificate error occurs when connecting to FortiAnalyzer via SSH
1194232	System stalls during reboot with IPv6 traffic due to an error condition in the scheduling daemon.
1194982	Interface bandwidth becomes zero when fast path is enabled
1196312	High CPU usage occurs when forming IPsec tunnels to a central HUB over PPPoE interface on 50G and 70G models
1197255	Error condition in sflowd occurs when removing entries from netflow cache under high load
1197529	Unable to free memory local user authentication until fnbamd restarted
1197885	Memory usage issues caused by ASLR when upgrading from 7.4.7GA to 7.4.8GA
1198181	An error condition in SNMP daemon occurs when querying fgVpnSslStatsEntry after upgrading to 7.6.4
1198350	MTU inconsistency occurs when using redundant interface with Jumbo MTU
1198758	Intermittent traffic disruption occurs when using KPN SIM card with default APN settings.
1198772	High CPU usage issues observed during GTP traffic handling on multiple slave FPMs
1199132	An error condition occurs in the lan-extension-controller when changing the controller address.
1199169	IPv6 address acquisition issues occur during upgrade to v7.6.4
1199322	VDSL2 sync issue occurs when ITU G.993.5 is enabled on 50G-DSL
1199648	Traffic interruption occurs when shutting down an interface in a dual inter-crossed connection with Hardware Switch
1200220	Intermittent disconnection of FortiAnalyzer from FortiGate caused by excessive TPM requests from httpsd.
1200320	VPN goes down when dhcpc tries to renew IP lease and receives a DHCPNAK response.
1200604	Config backup to FortiGate Cloud fails when retrieving full config.
1203193	FGR-70G and FGR-70G-5G-Dual do not support CLI for automation-stitch notifications when DIO module alarm functionality is activated, namely, 'set condition-type input' is not available under 'config system automation-condition'.

Bug ID	Description
1204023	SNMP response contains wrong values when querying certain OIDs under FgSoftware
1204631	CPU usage issues observed during snmpd operation
1205316	Recurrent disconnections occur when IMS APN attachment attempts are made
1206778	Unable to update FortiGuard licenses when file permissions are inccorect
1207768	FortiGate set the most significant bit of the sequence number to 1 in GTPv2 Delete Session Request after tunnel timeout
1209720	LAN 1, 2, 3, and A speed LED issues occur during NIC-led test step 3.
1209793	Interface configuration loss occurs when FortiGate reboots after a power cycle
1211645	Authentication error when using HEX based keys with SHA1 or SHA256 in NTPv4
1211647	Authentication error when using SHA256 as key-type in NTPv4
1211704	Time synchronization issues occur when NTP server authentication is enabled
1211873	Device connection state is not updated when connected to FortiGate integrated hardware switch on platforms with no logdisk.
1213371	Duplicate 0.0.0.0 entry occurs when adding existing secondary IP address on CLI
1214384	Unexpected behavior in FortiGate occurs when processing IPv6 traffic with invalid destination entries.
1214950	Batch mode configuration of system admin is allowed without specifying admin credentials
1215780	Connection failure occurs when using a custom APN
1216658	Packet drop occurs when traffic is initiated from the Internet to devices connected to the EMAC VLAN interface
1217130	VDOM removal occurs from dia sys vd list output when rebooting FortiGate with dedicated-mgmt enabled
1217366	Port speed mismatch occurs when setting speed to 1000MB on port1~port8
1217722	CPU usage issues observed when dedicated-management-cpu is enabled on np6 platform
1217924	Packet size issues occur when 802.1AD interface is based on a LACP interface with MTU set to 9216.
1218596	Error condition in cmdbsvr daemon occurs when changing opmode
1220898	FortiGate becomes unresponsive when adding more than three 802.1ad interfaces
1220984	Incorrect time stamp in FortiSentry log files occurs when 700G NPI merge happens
1221196	Optical port speed issues occur when connecting to Ericsson or Nokia radio nodes on FortiGate 90G/91G.
1221738	Returning packet is not forwarded via the expected LACP interface when set algorithm L3
1221994	CPU usage issues observed during TX direction port mirroring

Bug ID	Description
1222523	need 100full and 100auto speed settings for port17-24 on FortiGate 120G/121G
1223295	MTU override size inconsistency occurs when changing mtu on aggregate interface with emac-vlan
1227507	Support multiple geneve interfaces with the same underlying physical interface to be members of same software switch
1228304	Unexpected behavior occurs when FortiGate receives Forward Relocation Request without PDN IE message
1228420	PCI device check fails when BIOS version is 07000203
1228807	Some secret keys are not updated after a config change even when Private-Data-Encryption is enabled
1228992	Memory usage issues caused by exceeding device memory quota
1229804	Unexpected behavior occurs in the system when handling ICMPv6 host unreachable error messages after IPv6 neighbor entry expires
1229917	Same help text is displayed for clear and append commands when configuring system zone setting
1230471	An error condition in the firewall occurs when transmitting large packets over VXLAN and IPsec.
1231510	IP address assignment issues occur on DSL interfaces configured with static IP after reboot or at irregular intervals
1231940	For FortiGate using legacy BIOS version 04000006, the system may fail to reach the Serial Number for BIOS during boot up.
1233869	Unexpected behavior in the system occurs when disk logging is enabled
1234908	Traffic loss occurs when softirq spikes on FortiGate
1235359	Slowness occurs when renaming address objects
1238186	Error condition occurs when BGP neighbors are configured and IPv6 DHCP Client is enabled on WAN interface
1238520	Registration bypass option is available during the 7-day setup period
1239336	Central management configuration issues occur when using FortiGate GUI for Forticare registration
1240904	An error condition occurs in SNMP when querying fgNPUTables on FortiGate 201G with NP7LITE Processor
1244037	Limited speed options occur on 1G RJ45 ports of FortiGate 200F and 201F.
1244259	Console becomes unresponsive due to being overwhelmed by excessive logging when cpu stalls occur.
1246081	Memory usage issues caused by running v4/v6 routing protocols
1246315	An error condition in snmpd occurs when querying fgLicVersion

Bug ID	Description
1246914	Unexpected behavior in the kernel occurs when forwarding ICMP error messages from NAF devices
1248244	Memory usage issues caused by slab size configuration on low-memory FortiGate devices
1249410	Incomplete data erasure occurs on FortiGate-60F when executing erase-disk SYSTEM command
1255825	Conserve mode may occur when running full Security Rating report devices that have hundreds of extension devices (such as FortiAPs).
1255973	CPU usage issues observed during GUI session queries
1257295	An error condition occurs when both g-Fortinet_SSH_ECDSA256 and Fortinet_SSH_ECDSA256 exist simultaneously.
1261088	An error condition in the connection daemon occurs when configuring a broadcast IP address on a FortiGate interface via CLI
1261999	Interfaces are deleted when VLAN interfaces with different forward-domains are added to the same zone.
1263001	IPsec dial-up instability occurs over WWAN interface on FortiGate 51G after upgrading from 7.4.9 to 7.4.11
1264495	Throughput drops to 0 during netperf testing on FGT200G and FGT201G.
1266447	Inconsistent values occur when querying SNMP OID 'fg5gMdmOpMode'
1267113	LLDP advertised Sysname truncation occurs when a local domain is configured
1267635	An error condition occurs in the system during disk scan execution
1268947	High CPU usage occurs when creating or editing a VLAN interface via the web UI
1271792	Failover to secondary IP does not occur when primary Fgfm connection is down

Upgrade

Bug ID	Description
1135049	An error condition in ips_load_json_gzfile occurs during FortiOS same image upgrade
1152422	Enhance security by upgrading OpenSSH version
1155333	FGT/FWF-3XG upgrade fails with error "inflate failed: round 1, err -3" when memory usage is high
1158947	Manual patch upgrade not allowed when system has invalid upgrade license
1193036	Inconsistency occurs when auto-firmware-upgrade-start-hour default value is checked

Bug ID	Description
1243233	Configuration load failure occurs when upgrading to 7.6.5 through FortiManager
1250292	From a FGT-121G, upgrading a fabric device FSW-T1024E fails
1252663	On FortiGate D-series devices running older BIOS versions, the serial number changes to FGT0000000000001 after upgrading to FortiOS 7.4.10,7.4.11,7.6.5,7.6.6.
1256067	Required automatic upgrade may not complete successfully when device is unlicensed or end-of-support.

User and Authentication

Bug ID	Description
1112301	CPU usage issues observed during certificate authentication with multiple DNS replies
1118212	Captive portal authentication fails after FortiToken push notification approval during radius authentication with FAC for remote groups.
1122979	Custom NAS-ID not sent to RADIUS server when testing connectivity via GUI.
1134368	LDAP server becoming unreachable 'set mfa-mode subject-identity' is configured under the user peer settings, or ha-direct enabled with source-ip.
1137727	Delays in SSH login verification occur on some FortiGate models when hashing passwords, and immediate failure messages are returned for invalid usernames.
1139688	Username truncated when RADIUS Accounting-Request username exceeds 66 characters
1142387	SCEP enrollment fails when using IP address to connect to the server.
1144487	CPU usage issues observed during high load on fnbamd
1146635	Fnbamd issu during certificate authentication when multiple DNS replies contain both IPv4 and IPv6 parts.
1147049	Device hostname is not displayed when device identification is enabled and mDNS includes the device UUID.
1148209	Auto-enrolment for EC certificate using SCEP fails when reading inner PKCS#7
1156903	CLI authentication test fails when RADIUS server has require-message-authenticator setting disabled.
1158484	When user logs into the FortiGate via FortiManager's CLI console, users are not forced to change password even if password has expired.
1163152	RADIUS stops working on secondary unit when HA secondary connects to a Radius server using UDP.

Bug ID	Description
1165116	Event log is not generated for expired authentication attempts, like when it fails due to 2FA timetout
1169349	Assignment of FortiToken through FortiManager fails when FortiGate is configured.
1170894	IKEv2 local user authentication issues occur when using two-factor email authentication with extended timeout values
1177318	Factory default certificates not displaying certificate information in the CLI for FortiGate-201G models
1177519	Login failure occurs when attempting to access admin user without a username query parameter
1177593	User addition fails with FortiToken Cloud when using 2 HA FortiGates with virtual serial number enabled
1178467	Administrator accounts are unintentionally unlocked when the admin-lockout-threshold is increased.
1181737	Missing optional fields occur during CSR SCEP Enrollment with Entrust CA
1182725	EAP-proxy fails to match group when the group length exceeds 128 characters
1185705	Seed import failure occurs when uploading token seed file via GUI
1189693	LDAP authentication fails on OpenLDAP due to the type of ldap_result used.
1193697	Emails with FortiToken codes are not sent due to an SSL error when using SMTPS port 465
1196434	SAML authentication issues occur when LASSO_PROFILE_SIGNATURE_VERIFY_HINT_FORCE is set and the SAML response is not signed.
1205671	Authentication failure occurs when all-usergroup is enabled under radius
1207282	Authentication failure occurs when using multiple wildcard entries for admin access with TACACS server
1213932	SAML authentication issues occur when authd encounters an error condition during IPsec SAML SSO authentication
1214438	Failover to secondary Tacacs+ server occurs when primary server is unreachable.
1217617	Login failure occurs when a trusted host is set for the admin after upgrading FortiGate to version 7.4.9
1218458	Hardware token activation fails when CMDB write permission is enforced.
1223051	Authentication failure occurs when using remote RADIUS server with TFA enabled
1228793	Certificate auto-enrollment via CMPv2 fails when using an intermediate CA cert after upgrading
1239951	Hardtoken activation fails when CMDB write permission is enforced
1243758	SCEP enrollment fails when sending GetCACaps request without CA name mark due to server error

Bug ID	Description
1244268	Fnbamd error when downloading intermediate CAs through multiple AIA links
1246613	Radius CoA disconnection fails when sending a CoA Disconnect Request with a Calling-Station-Id on FortiOS 7.6
1247109	Authentication issues occur when editing a vdom CA certificate with VDOM enabled
1251941	An error condition occurs in EAB when entering an HMAC value with a 66-byte key.
1259154	Authentication failure occurs when certificate rotation happens on Standalone HA primary FortiGate
1263865	Connection failure occurs when maximum session limit is reached with EAP enabled in IKE config and TFA for users.

VM

Bug ID	Description
1041341	Error condition occurs when using vlink0 with HTTPS on FGT-VM-AZURE
1102434	Configuring VRF on hbdev will cause FortiGate VM HA not Syncing
1125437	The "set distance" option under interface configured as dhcp client doesn't work o vm
1157674	Incorrect system time occurs when FortiGate-VM64-GCP boots up on GCP
1159433	DPDK error when traffic reaches more than 4GBps
1161380	License becomes invalid when system time is incorrect on FortiGate VM64-GCP devices
1172050	Packet-rate information is missing for some interfaces when running the diagnose netlink interface packet-rate command on FortiGate-ARM64-AWS.
1194713	ARM_KVM/GCP/OCI unable to format shared data partition on ARM VMs
1195615	Failover issue occurs when reserved IP address exists in an OCI subnet and is not associated with a VNIC.
1198515	Memory usage issues caused by IPsec tunnel rekey when DPDK is enabled
1204790	IP address collection issues occur when a VM reports a provisioning error in a VMSS
1207410	Port flapping occurs when using iavf driver
1213875	License download failure occurs when using proxy setting for Azure and AWS PAYG.
1215317	Public IP disassociation occurs when SDN connector uses wrong Azure Management API endpoint
1215396	Unexpected behavior occurs when configuring a VLAN sub-interface on a physical port with DPDK enabled

Bug ID	Description
1217942	FQDN synchronization issues occur when the primary's timeout value on the secondary is not refreshed in a timely manner.
1219012	Dynamic object updates fail when an SDN connector is not functioning
1220070	Discrepancy in interface stats occurs when COS is set and DPDK offload is enabled
1221924	Inconsistency in IPS-socket size occurs when using a subscription license
1223933	Loss of VWP configuration occurs when rebooting with unreferenced member interfaces
1224484	An error condition occurs in the diag daemon during image upgrade matrix operations
1228324	Azure SDN connector fails to update new subscriptions until restarted.
1239551	Image publishing issue occurs when signing shim bootloader with Fortinet CA on Azure
1245936	FGT-VM failed to validate vm license from FortiManager with ipv6 address
1265185	Configuration divergence occurs when set private-ip is present in SDN Connector configuration
1266927	License validation issues occur when FortiGate-VM64 is behind a proxy in a closed network
1269889	Dynamic objects are removed when FortiGate encounters a 503 Service Unavailable from Google Cloud Platform.
1272991	Boot up failure occurs when confidential VM is enabled
1274753	License status warning occurs when secondary FortiGate validates VM License after upgrading to v7.4.11 or v7.4.10

VoIP

Bug ID	Description
1201825	Packet drop occurs when SIP ALG and Hyperscale are enabled
1204573	Calls fail to establish when FortiGate receives a SIP 302 Redirect response from a Load Balancer.
1227757	Unexpected RTP stream closure occurs when provisional-invite-expiry-time is reached

Wan Optimization

Bug ID	Description
1160444	Global config wanopt content-delivery-network-rule is deleted when restoring vdom config
1252420	An error condition in WAD occurs when ignore-pnc is enabled for webcache and a HTTPS request is sent with a Pragma: no-cache header.

Web Application Firewall

Bug ID	Description
1130819	Registration traffic is blocked when WAF profile is enabled
1208919	Credit card information detection issues occur when WAF credit card signature requires PCRE_MULTILINE.

Web Filter

Bug ID	Description
1074960	Internet connectivity slowness may occur in proxy-mode inspection policies due to traffic cannot fully utilize queues from all NPUs.
1096297	Timeout occurs when web filter is enabled and fragments occur
1096442	Web filter logs are not displayed when offload is enabled in the Policy
1098739	[Combine with mantis 1159041] SSL errors occur when accessing certain websites via IPv6 in FortiGate flow mode with SSL inspection enabled.
1116052	In some cases, incorrect session blocking may occur when a URL rating query fails during security policy matching in NGFW policy mode.
1141367	Intermittent traffic disruption occurs when using Safari browser with proxy-based inspection and certificate inspection enabled.
1150232	Threat feed URLs are not blocked since Sandbox block list file version check was always failed and aborted loading of other types of URL list including External-resource category URL list
1156789	Web filter settings category name, block screen category name, and log category name are translated into different Japanese when using web filter profile on FortiGate.

Bug ID	Description
1156979	[Combine with mantis 1159041] SSL errors occur when accessing certain websites via IPv6 in FortiGate flow mode with SSL inspection enabled.
1158138	Some websites may fail to load when the web filter is enabled due to the server setting an initial window size that is too small
1158586	[Combine with mantis 1158138] Some websites may fail to load when the web filter is enabled due to the server setting an initial window size that is too small
1158993	[Combine with mantis 1158138] Some websites may fail to load when the web filter is enabled due to the server setting an initial window size that is too small
1166666	Domain fronting block occurs when sending traffic with upper case domain name over HTTP 1.1
1168879	Dynamic content on webpages failed to load when the proxy layer was enabledspecifically when WebFilter Safe Search or Strip-XFF options were active.
1177015	Webfilter logs are not generated when https-replacement-message is disabled in proxy-policy with DPI
1184183	Duplicated webfilter logs occur when "log-all-url" is enabled in NGFW policy mode, causing redundant entries for each traffic event.
1185240	IP address is added to custom header when http-ip-header is enabled on virtual server and custom header value starts with 'a' (v7.4.8) or 'h' (v7.6.4).
1205450	SSL/TLS errors and latency occur when using local threat feed URL category in NGFW policy mode
1208074	Translation issues occur when FortiGate GUI is set to Portuguese
1211319	URL filter issues occur when using perl style regex flags after upgrade
1214017	Memory usage issues occur when adding an external threat feed with a large number of similar patterns
1227049	YouTube channel main page cannot be blocked by channel filter when proxy-inline-ips is enabled
1229941	Webfilter logs are not generated correctly when FortiGate is in NGFW mode with policy-based configuration.
1230414	Improvements to resolve memory usage issues when logical-sn is enabled
1232698	Antiphish fails to block usernames with '.' character when enabled.
1241179	Video downloads using Wondershare UniConverter stall or stop mid-process when FortiGate's web filter encounters out-of-order packets during transfer.
1254458	Authentication page is not displayed when webfilter category is set to authentication action
1268027	Video blocking issues occur when accessing YouTube from the main page with channel filters

WiFi Controller

Bug ID	Description
1001211	Add optional antenna support for K-series models 443K and 243K
1127637	wpad requests are sent exclusively to IPv6 addresses and do not attempt fallback to IPv4 in environments supporting dual-stack configurations.
1145326	In non-root VDOM, device fails to authenticate when MPSK is used with an external RADIUS server
1147416	Connection fails for Samsung S22 devices when using WPA3-SAE from local-radio on certain FortiGate models.
1151713	FortiAPs may go offline when memory pool of WiFi daemon cw_acd is fully occupied and not released properly. cw_acd debug constantly show ERR: NO MEM for USER_LOCAL_MSG workaround: kill the cw_acd process manually diag system kill 9 <pidofcw_acd>
1158619	6GHz channels 1 to 93 are not available when AP-Country is set to Hungary
1158774	Wireless and wired devices cannot communicate across a software switch on FortiGate-G models when capwap-offload is enabled. This issue affects deployments attempting to create a flat Layer 2 network between wired and wireless segments.
1161023	Groups of Wi-Fi clients are lost after roaming to a different AP, causing unintended behavior in network policies.
1165690	The cw_acd process on the FortiGate may exhibit high CPU usage when Radio-3 is dedicated to monitor mode and perform rogue AP scanning.
1174782	The client fails to authenticate and gets disconnected from the access point when initiating Fast BSS transition (FT) roaming with MAC authentication enabled.
1177859	When FWF local radio is in non-root vdom, wifi users encounter connectivity issues
1180552	Logs display incorrect channel ID after DFS detection.
1189187	The AP profile's auto-transmit power range adjusts unexpectedly when a single endpoint is modified.
1191723	Wireless clients encounter VLAN flapping between NAC and onboarding.
1192905	FortiGate not honouring VRF-Select for self-originating traffic - WIFI Radius authentication
1192914	WiFi SSID signal loss may be observed after multiple power cycles on FWF FortiGate models.
1207256	Inconsistent client signal-to-noise ratio values occur on some FortiGate models.
1209209	FortiGate devices fail to process authentication responses during IKEv2 setup, resulting in connection failures.
1213368	AP information is missing from forward traffic logs (of captive-portal SSID)

Bug ID	Description
1217779	An error condition in cw_acd occurs when dedicated-mgmt is enabled
1218025	Radius COA functionality does not work as intended when using an FQDN radius server with WiFi 802.1x authentication.
1219415	Connection failures may occur when WiFi clients authenticate using 802.1X and multiple IP addresses are resolved for the RADIUS server FQDN.
1221283	Clients unexpectedly keep moving between FAPs after frequency handoff from 5G to 2.4G due to obsolete BTSM request
1227978	Wi-Fi clients cannot maintain previous IP addresses after roaming from one FAP to another in the inter-controller layer-3 roaming topology.
1230455	SSID loss occurs on FortiGate models when DARRP channel optimization fails.
1232763	WiFi clients experience initial connectivty and packet-loss during roaming only on WPA2-Enterprise SSID with External RADIUS
1240269	The virtual MAC address of Tunnel VAP interfaces changes unexpectedly after FortiGate HA failover or reboot when adding a wireless-controller.vap with quarantine disabled.
1243404	Roaming fails when 802.11r is enabled on WPA2-Enterprise with invalid PMKID
1243456	FT reassociation fails when 802.11r is enabled on WPA2-Enterprise
1256821	The class attribute fails to restore when a Wi-Fi client roams between FortiGate access points using 802.11r.

ZTNA

Bug ID	Description
987129	Access denied occurs when favicon.ico is sent by browser during ZTNA SSH session with SAML auth
1089157	An error condition in WAD occurs when adding a ztna-ems-tag to a proxy policy with an active ZTNA session
1102925	Memory usage issues caused by accessing multiple websites through WAD
1117660	ZTNA forwarding fails when using FQDN myztna.com.local.ca as proxy gateway
1134649	WAD cannot re-verify new ems-tag after an ems-tag update for HTTPS access proxy, causing existing sessions to remain active despite matching a deny policy.
1135441	CLI error occurs when configuring SAML server in api-gateway with access-proxy6 and vip6 configured.
1139201	Internal resources are inaccessible via IP or FQDN when using agentless ZTNA Access proxy-portal with apptype web on FortiGate.

Bug ID	Description
1159018	ZTNA agentless not working on FG-90G devices.
1172396	The Certificate Information field in the replacement message shows incorrect information when ZTNA access proxy is configured to accept empty cert.
1178076	When access proxy is configured, client cannot access multiple virtual hosts on the same connection
1178742	ZTNA destination unreachable in rare cases where 'sni-server-cert-check' is enabled on a FortiGate and the SNI field is missing.
1183544	Portal displays wrong layout when accessing Agentless ZTNA web bookmarks with complex URLs
1184250	ZTNA access failure occurs when using a wildcard FQDN on the first attempt
1194525	Traffic blockage occurs when ZTNA UDP forwarding with deep-inspection is enabled
1198173	An error condition occurs in WAD when using ZTNA portal RDP web bookmarks.
1199808	Incorrect policy type recorded on ZTNA traffic logs
1208519	Traffic is denied when accessing HTTPS bookmarks with subdomains of the ZTNA Portal's root domain
1229620	Redirect failures occur when VIP ports do not match real server ports
1253873	SNAT failure occurs when ZTNA access-proxy policy uses IP pool
1254981	Error condition in WAD occurs when ZTNA proxy with SAML authentication for RDP is used without daily restarts.
1257675	Connection error when didn't set sso and didn't set username and password for VNC bookmark when connecting to UltraVNC server
1272422	File uploads fail when using ZTNA Web Portal SMB bookmarks after ECO 293909

Known issues

Known issues are organized into the following categories:

To inquire about a particular bug or report a bug, please contact Customer Service & Support.

New known issues

The following issues have been identified in version 8.0.0.

AntiVirus

Bug ID	Description
567417	Eicar passes when two security policies are configured, first one denies application and second one enables AV scan. **Workaround**: Use wildcard policies to block AV reliably

DNS Filter

Bug ID	Description
1254680	DNS-over-TLS fails when configured on FortiGate 201E with FortiOS 7.4.10 **Workaround**: Set ocsp-status to disable or set ocsp-option to server and use an IP server in config vpn certificate setting.

Firewall

Bug ID	Description
1254541	IPsec tunnels and offloaded sessions restart when a QoS profile is configured

FortiGate 6000/7000 Platform

Bug ID	Description
1250240	Traffic disruption occurs when kernel routes are not synchronized across the FPM. **Workaround**: Run diag test application chlbd 3 on the slot that's missing routes to trigger a manual routes redownload.

GUI

Bug ID	Description
1058668	Export to CSV/JSON file fails when policy number exceeds 700 due to non-existent application id **Workaround**: Remove the non-existent application IDs from the security policies
1102594	HA status on the Global Dashboard changes unexpectedly during hard refresh
1190683	Fabric Connector status shows as DOWN in GUI after failover on Azure SDN Connector cluster **Workaround**: Logout and login again to the GUI
1194972	Devices are not visible on Asset & Identities > OT view when API response from /api/v2/monitor/user/device/query retrieves devices without sufficient information.
1205102	Traffic logs cannot be viewed when Resolve unknown applications is enabled **Workaround**: Disable Resolve unknown applications under the global settings of log settings
1228366	Network interfaces are displayed in incorrect order when accessing Network>Interfaces on FortiGate 30G.
1232828	Unresponsive GUI occurs when httpd is fully loaded on the forward traffic page **Workaround**: Disable Resolve unknown applications in the log settings
1249752	Incorrect HA status occurs when switching to mgmt-vdom vdom on FortiGate-6001F
1260292	Print button is not visible when using prof_admin profile after FortiOS upgrade
1261462	Error saving request object to CLI occurs when editing copied ISDB policies with FQDN address in destination
1262047	Connection loss occurs when web-svc-perf is enabled under log settings **Workaround**: Disable web-svc-perf under log setting
1262347	Multiple clicks are required to configure wildcard URL filters from the GUI **Workaround**: Select the wildcard first and then enter the URL
1265107	Blank page displays in GUI when vdom_admin logs in but lacks root access
1265177	Display issues occur in FortiView widgets when FIPS-CC mode is enabled **Workaround**: Create another super-admin profile to assign to the new admin.

Bug ID	Description
1265862	On FortiFirewall, GUI displays incorrect log traffic status when firewall policy is configured via CLI **Workaround**: Use set logtraffic all/disable instead of unset logtraffic
1271369	SAN format options are not available in GUI when creating a CSR on FortiGate **Workaround**: Use the following format for SAN entries when generating a CSR: DNS:example.com for DNS entries and IP:x.x.x.x or IP Address:x.x.x.x for IP addresses.
1274070	File name does not update with CLI console name when renamed
1274560	Non-resolvable FQDN objects intermittently show a red box around the object name when filtered by FQDN type in the Policy & Objects section on FortiGate.
1276291	Firewall Users Method and User Group graph disappears when using FortiGate v7.4.11

HA

Bug ID	Description
1205727	Gratuitous ARP exceeds configured interval when HA failover happens.
1246177	Warning pop-up is not displayed on FGCP cluster members in clusters with more than 2 members
1249251	TCP session failover fails when using NGFW policy-based mode after HA failover.
1273324	SNAT uses incorrect IP address after HA failover **Workaround**: Delete and re-add the secondary IP configuration manually

IPsec VPN

Bug ID	Description
1238675	Connection fails to establish when FortiClient VPN Android connects to FortiGate IPsec IKEv1

Log and Report

Bug ID	Description
1265088	Syslog packets are sent when syslog-override is enabled
1266492	Secondary unit logs are not received by FortiAnalyzer Cloud when running FortiOS 7.4.9 and above in a FortiGate HA cluster

REST API

Bug ID	Description
1265839	Group Filter functionality is impacted when a large number of users are authenticated.
1267118	Filters are ignored when using the /firewall/sessions API call

Routing

Bug ID	Description
1260891	BFD packet transmission issues occur when a port member of the aggregate interface is shut down and then brought back up on the switch side. **Workaround**: Change bfd-detect-mult to 7 on both sides.

Security Fabric

Bug ID	Description
995772	Devices are missing from Asset identity center / OT View when API response from /api/v2/monitor/user/device/query retrieves devices without sufficient information.

Switch Controller

Bug ID	Description
1187046	FortiGate fails to detect FortiLink-HTTPS tunnel mode when FortiLink interface is enabled
1275148	Allowed VLANs are deleted when adding new allowed VLANs on a trunk port.

System

Bug ID	Description
1179827	Hardware switch configuration limitations occur when adding Wan1 and Wan2 on FortiGate
1190222	Incompatibility occurs when using 8G eMMC on 3XG/5XG/7XG/9XG models

User and Authentication

Bug ID	Description
1241530	LDAP authentication fails when password is not sent in bind request

VM

Bug ID	Description
1115988	Security Fabric Connector and Firmware and Registration pages display incorrect registration status when loading FortiFlex VM license **Workaround**: Reboot the system to resolve the issue

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 8.0.0.

FortiGate 6000/7000 Platform

Bug ID	Description
947982	Audio cutouts occur when CG_FULL errors are high on NP7 models
1130491	Traffic disruption occurs when WCCP is enabled on FortiGate **Workaround**: Direct all related traffic to master FPC

GUI

Bug ID	Description
1237136	Dynamic VLANs are not visible on the GUI when a port-security-policy is applied

HA

Bug ID	Description
1226122	System > HA: There is no "upgrade" button on secondary GUI page when HA in "local-only" or "secondary-only" MVC upgrade mode **Workaround**: is to upgrade the secondary via the command line

HyperScale

Bug ID	Description
1200885	Renaming an ippool in a FortiGate setup with VDOMs results in unintended behavior affecting network traffic.
1219541	Traffic disruption occurs when changing an interface's vdom **Workaround**: Use two static routes 0.0.0.0/1 and 128.0.0.0/1 as the default route instead of 0.0.0.0/0
1262881	Hw session sync dev goes out of sync due to the discrepancy in lag driver between primary and secondary

IPsec VPN

Bug ID	Description
1131269	UESP packet drop occurs when VPN peer uses different source ports for IKE-NATT and UESP **Workaround**: Add a flow rule to work around the issue

Built-in AV Engine

AV Engine 8.0014 is released as the built-in AV Engine.

Resolved engine issues

Bug ID	Description
908756	Add dumping support for InnoSetup 6.1.0
1136046	The engine cannot dump the InnoSetup 6.4 installer
1171494	CDR Missed Detection of Malicious PDF Link
1202717	PDF with embedded XML is corrupted after CDR

Built-in IPS Engine

IPS Engine 8.0028 is released as the built-in IPS Engine.

Resolved engine issues

Bug ID	Description
673117	Unexpected behavior occurs when FortiGate processes TFTP protocol data under certain conditions.
764143	SSL version restrictions not enforced in flow mode when using 'min-allowed-ssl-version'.
983372	An error condition in IPS engine occurs when accessing safebrowsing.google.com
1077638	In NGFW Policy Mode, FortiGate may incorrectly block packets from established TCP sessions if no matching IPS session exists.
1080003	FGT memory is gradually increasing when FGT Flow AV Profile is inspecting TCP 6200 traffic with outbreak prevention enabled.
1091118	Oversized packets exceeding the MTU cause delayed ACKs, leading to unintended behavior
1093769	Unexpected IPS UTM logs may be generated in NGFW policy mode for unknown applications.
1094030	URL truncation occurs in logs due to mismatched length limits between FortiOS and IPSEngine.
1094870	FTPS data connections fail to establish when using flow mode firewall policies configured for FTP service.
1096297	Timeout occurs when web filter is enabled and fragments occur
1107273	New packets on established SCTP sessions are dropped during processing after a four-way handshake when UTM is enabled.
1116052	In some cases, incorrect session blocking may occur when a URL rating query fails during security policy matching in NGFW policy mode.
1117043	Fatal errors occur when the IPS engine sends requests with zero-length data segments to IPSA.
1122188	Internal diagnostic commands fail or delay when ipsmonitor processes each request sequentially due to sequential forwarding to IPS daemon processes.
1129130	Intermittent traffic disruption occurs when FortiGate is in NGFW mode and it encounters traffic which are legitimate but do not create a session
1131911	Memory usage issue observed in IPSEngine 7.00560 during high SMTP traffic due to improper memory management.
1140846	Unexpected behavior observed in the IPSEngine when handling HTTPS traffic using HTTP/2 in

Bug ID	Description
	certain configurations.
1144684	High CPU usage occurs when processing multiple RTSP streams due to inefficient resource management by the RTSP decoder.
1150204	File attachment names from naver.com are displayed as 'uploadByXHR' instead of their actual filenames
1152040	An error condition occurs in custom IPS signature when using --log after upgrade to 7.4.5
1152384	CPU usage issues observed during intense IPS packet scanning
1156180	Unexpected behavior observed in the IPSEngine caused by an invalid numeric entity.
1156490	When inspection mode is proxy, inspect-all is enabled and http-policy-redirect is enabled, traffic is not sent to WAD for processing and consequently dropped
1158138, 1158586, 1158993	Some websites may fail to load when the web filter is enabled due to the server setting an initial window size that is too small
1158524	Unexpected behavior observed in the IPSEngine when a DNS packet matches a policy with DNSFilter and Safe Search enabled.
1098739, 1156979, 1159041	SSL errors occur when accessing certain websites via IPv6 in FortiGate flow mode with SSL inspection enabled.
1159485	Traffic duplication may occur on FortiGate due to retransmission of out-of-sync TCP streams when insecure ciphers are used.
1162794	Unintended behavior occurs in the IPS Engine caused by the SCADA dissector.
1168037	Error condition occurs in proxy mode when using inspect-all certificate-inspection in ssl-ssh-profile
1168879	Dynamic content on webpages failed to load when the proxy layer was enabledspecifically when WebFilter Safe Search or Strip-XFF options were active.
1169917	Websites may fail to load when inspectall certificate inspection and application control are enabled in proxy mode after upgrading to a build that supports Encrypted ClientHello (ECH)
1170304	Websites load slowly when NPU offloading is enabled in firewall policy and the packet length is bigger than the MSS due to many fragmentation needed packets
1178184	SSL errors occur when accessing a specific website due to an unexpected record type when Web Filtering and DPI are enabled in Flow mode.
1178742	ZTNA destination unreachable in rare cases where 'sni-server-cert-check' is enabled on a FortiGate and the SNI field is missing.
1181573	SSL inspection does not correctly add the Authority Key Identifier (AKID) when operating in Flow mode with DPI enabled.
1182461	High memory usage occurs when multiple HTTP2 connections with many open streams are present.

Bug ID	Description
1184183	Duplicated webfilter logs occur when "log-all-url" is enabled in NGFW policy mode, causing redundant entries for each traffic event.
1190395	Intermittent traffic disruption occurs due to an error condition in the IPS Engine caused by a DAC handler issue.
1191598	High CPU usage occurs when HTTP2 connections have a large number of open streams
1193876	Memory usage issues caused by improper closure of HTTP2 streams
1197659	An error condition in IPS engine occurs when processing HTTP traffic
1205692	FTP traffic is blocked when Application Control is enabled over Sock5
1210836	Conserve mode occurs when IPSEngine memory usage increases due to gradual increase in AnonPages.
1212296	Package download failure occurs when IPS profile is enabled
1213957	TCP download rate drops when FortiGate uses SSL inspection with an antivirus profile in flow mode.
1216974	Intermittent traffic disruption caused by an error condition in the IPS Engine during hybrid key generation.
1217478	Incomplete IEC 60870-5-104 detection occurs when IPS session is cleared.
1218520	BFD flaps occur due to an error condition in the IPS engine caused by QUIC traffic.
1219051	MSI files are not blocked when downloaded in flow mode
1225743	An error condition in IPS Engine occurs when executing ssl_add_defer_log during stress testing
1229928	Traffic is not blocked as expected when DNS response returns NXDOMAIN in flow-based mode
1229941	Webfilter logs are not generated correctly when FortiGate is in NGFW mode with policy-based configuration.
1239080	Abnormal traffic log behavior occurs when FortiGate is running in sniffer mode with ips-sniffer-mode enabled.
1241179	Video downloads using Wondershare UniConverter stall or stop mid-process when FortiGate's web filter encounters out-of-order packets during transfer.
1249177	High CPU usage occurs when IPSEngine scans SMB traffic
1252636	An error condition in IPS Engine occurs when upgrading to v7.6.6
1253472	Unexpected behavior observed in the IPS Engine during HTTP header processing involving buffer edit cases on FortiGate models.
1260248	Protocol Enforcement fails to block DNS over TCP traffic when non-DNS TCP traffic uses port 53
1269354	An error condition in IPS engine occurs when handling unusual TLS 1.3 stacks.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com