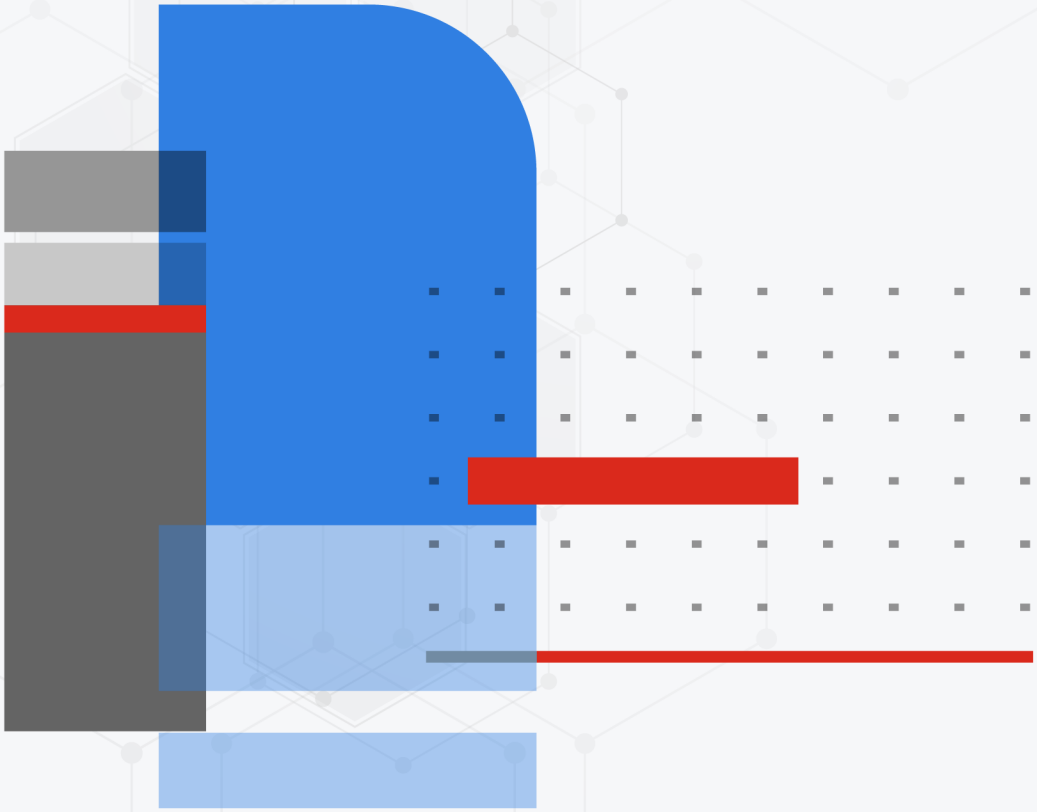
Release Notes

FortiOS 7.4.9



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

September 29, 2025
FortiOS 7.4.9 Release Notes
01-749-1181283-20250929

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-09-25	Initial release.
2025-09-29	Updated New features or enhancements on page 16, Resolved issues on page 31, Known issues on page 48, and Built-in IPS Engine on page 58.

Introduction and supported models

This guide provides release information for FortiOS 7.4.9 build 2829.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.4.9 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-50G, FG-50G-5G, FG-50G-DSL, FG-50G-SFP, FG-50G-SFP-POE, FG-51G, FG-51G-5G, FG-51G-SFP-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-70G, FG-70G-POE, FG-71F, FG-71G, FG-71G-POE, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-DSL, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-90G, FG-91G, FG-100F, FG-101F, FG-120G, FG-121G, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-200G, 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-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-50G, FWF-50G-5G, FWF-50G-DSL, FWF-50G-SFP, FWF-51G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, 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-OPC, FG-VM64-RAXONDEMAND, FG-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.4.9 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

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.4.9 features.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.4.9 features.

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

SMB drive mapping with ZTNA access proxy

In FortiOS 7.4.1 and later, SMB drive mapping on a Windows PC made through a ZTNA access proxy becomes inaccessible after the PC reboots when access proxy with TCP forwarding is configured as FQDN. When configured with an IP for SMB traffic, same issue is not observed.

One way to solve the issue is to enter the credentials into Windows Credential Manager in the form of `domain\username`.

Another way to solve the issue is to leverage the KDC proxy to issue a TGT (Kerberos) ticket for the remote user. See ZTNA access proxy with KDC to access shared drives for more information. This way, there is no reply in Credential Manager anymore, and the user is authenticated against the DC.

Local out traffic using ECMP routes could use different port or route to server

Starting from version 7.4.1, when there is ECMP routes, local out traffic may use different route/port to connect out to server. For critical traffic which is sensitive to source IP addresses, it is suggested to specify the interface or SD-WAN for the traffic since FortiOS has implemented `interface-select-method` command for nearly all local-out traffic.

```
config system fortiguard
    set interface-select-method specify
    set interface "wan1"
end
```

Hyperscale NP7 hardware limitation

Because of an NP7 hardware limitation, for CGN traffic accepted by a hyperscale firewall policy that includes an overload with port block allocation (overload PBA) IP Pool, only one block is allocated per client. The setting of the hyperscale firewall policy `cgn-resource-quota` option is ignored.

Because of this limitation, under certain rare conditions (for example, only a single server side IP address and port are being used for a large number of sessions), port allocation may fail even if the block usage of the client is less than its quota. In cases such as this, if the client has traffic towards some other servers or ports, additional port allocation can become successful. You can also work around this problem by increasing the IP Pool block size (`cgn-block-size`).

Changes to NP7 traffic shaping

The following known issues for the Queuing based Traffic Management (QTM) module on NP7 are fixed:

- Incorrect checksum for fragments after QTM.
- Packets longer than 6000 bytes cause QTM to hang.
- Refreshing causes QTM to hang.
- MTU is not honored after QTM, so the packet is not fragmented.

As a result of these changes, you can no longer use the following command to change QoS type used for traffic shaping for sessions offloaded to NP7 processors:

```
config system npu
    set default-qos-type {policing | shaping}
end
```

Instead, `default-qos-type` can only be set to `policing`.

For NP7 sessions, policy traffic shaping, per-IP shaping, and regular port shaping (outbandwidth enabled on an interface without a shaping profile) always use the NP7 accounting and traffic shaping module (called the TPE module). This is the same as changing the `default-qos-type` to `policing`.

For NP7 sessions, shaping profiles on interfaces now only use QTM for traffic shaping (equivalent to setting `default-qos-type` to `shaping`). Shaping profiles on interfaces are also called Multiclass shaping (MCS). The interface can be a physical interface, LAG interface, and VLAN interface (over physical or LAG). The FortiGate supports shaping profiles on a maximum of 100 interfaces.

GUI cannot be accessed when using a server certificate with an RSA 1024 bit key

The GUI cannot be accessed when using an admin server certificate with an RSA 1024 bit key after upgrading to FortiOS 7.6.1, 7.4.8, or 7.2.11. An RSA key of at least 2048 bits is required. Certificates that are using an RSA key of less than 2048 bits are no longer supported.

SSL VPN not supported on FortiGate G-series Entry-Level models

The SSL VPN web and tunnel mode feature will not be available from the GUI or the CLI on the FortiGate G-Series Entry-Level models, including 50G, 70G, 90G and variants. Settings will not be upgraded from previous versions.

Consider migrating to using IPsec Dialup VPN for remote access. See FortiOS 7.4 SSL VPN to IPsec VPN migration.

FortiSwitch port page design change

Due to a FortiSwitch port page design change, the right-click popup menu is no longer available to configure some features, such as STP, BDPU, and edge port. A drop-down list is available instead. Beside the feature status of the desired port, click the *edit* icon to access the drop-down list and configure the feature.

SAML certificate verification

Starting from FortiOS 7.2.12, 7.4.9, and 7.6.4, FortiGate verifies the signature for SAML response messages. Please turn on *Sign SAML response and assertion* or similar options in corresponding IDP settings. Lack of signature for signing response messages or assertions may cause authentication to fail.

For more information on how the SAML response signing is configured, see Identify Providers.

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 initially supported on the FortiGate 900G series and FortiGate 200G series.

Changes in default values

Bug ID	Description
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.

Changes in table size

Bug ID	Description
1030001	On the 200-400 series FortiGates, increase the number of VDOMs from 10 to 25. On the 500-900 series FortiGates, increase the number of VDOMs from 10 to 50.
1129770	On High-End and Mid-Range FortiGate models, increase the number of IP addresses from 300,000 to 5,000,000 for High-End models and to 1,000,000 for Mid-Range models.

New features or enhancements

More detailed information is available in the New Features Guide.

Policy & Objects

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

Feature ID	Description
1108832	Adds support for displaying real-time traffic statistics in QTM, offering users a more intuitive and comprehensive view of traffic shaping performance across various interfaces on NP7/NP7Lite platform devices.

User & Authentication

See Authentication in the New Features Guide for more information.

Feature ID	Description
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 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.

VPN

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

Feature ID	Description
1057309	Dial-up IPsec with SAML using an external browser for authentication is supported starting from FortiOS v7.4.9, FortiClient versions 7.2.5 and 7.4.1 for Mac and Windows, and FortiClient version 7.4.3 for Linux.

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 17 and Upgrading Fabric or managed 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 7.4.9 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.4.8
FortiManager	• 7.4.8
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 or SSL 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 7.4.0, use FortiClient 7.4.0.

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 7.4.9. When Security Fabric is enabled in FortiOS 7.4.9, all FortiGate devices must be running FortiOS 7.4.9.

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 7.4.9:

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 7.4.9 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. Confirm that all components are synchronized and operating normally.
   For example, open the Cluster Status dashboard widget to view the status of all components, or use `diagnose sys confsync status` to confirm that all components are synchronized.

FortiGate 5001E primary blade failed to install image

SLBC FortiGate 5001E primary blade failed to install image, even though graceful-upgrade was disabled.

IPS-based and voipd-based VoIP profiles

In FortiOS 7.4.0 and later, the new IPS-based VoIP profile allows flow-based SIP to complement SIP ALG while working together. There are now two types of VoIP profiles that can be configured:

```
config voip profile
    edit <name>
        set feature-set {ips | voipd}
    next
end
```

A voipd-based VoIP profile is handled by the voipd daemon using SIP ALG inspection. This is renamed from proxy in previous FortiOS versions.

An ips-based VoIP profile is handled by the IPS daemon using flow-based SIP inspection. This is renamed from flow in previous FortiOS versions.

Both VoIP profile types can be configured at the same time on a firewall policy. For example:

```
config firewall policy
    edit 1
        set voip-profile "voip_sip_alg"
        set ips-voip-filter "voip_sip_ips"
    next
end
```

Where:

- `voip-profile` can select a `voip-profile` with `feature-set voipd`.
- `ips-voip-filter` can select a `voip-profile` with `feature-set ips`.

The VoIP profile selection within a firewall policy is restored to pre-7.0 behavior. The VoIP profile can be selected regardless of the inspection mode used in the firewall policy. The new `ips-voip-filter` setting allows users to select an IPS-based VoIP profile to apply flow-based SIP inspection, which can work concurrently with SIP ALG.

Upon upgrade, the `feature-set` setting of the `voip profile` determines whether the profile applied in the firewall policy is `voip-profile` or `ips-voip-filter`.

Before upgrade	After upgrade

`config voip profile`
`  edit "ips_voip_filter"`
`  set feature-set flow`
`  next`
`  edit "sip_alg_profile"`
`  set feature-set proxy`
`  next`
`end`
 	
`config firewall policy`
`  edit 1`
	`config voip profile`
	`  edit "ips_voip_filter"`
	`  set feature-set ips`
	`  next`
	`  edit "sip_alg_profile"`
	`  set feature-set voipd`
	`  next`
	`end`
	
	`config firewall policy`

Before upgrade	After upgrade
set voip-profile "ips_voip_filter" next edit 2 set voip-profile "sip_alg_profile" next end	edit 1 set ips-voip-filter "ips_voip_filter" next edit 2 set voip-profile "sip_alg_profile" next end

GUI firmware upgrade does not respect upgrade path in previous versions

When performing a firmware upgrade from 7.4.0 - 7.4.3 that requires multiple version jumps, the *Follow upgrade path* option in the GUI does not respect the recommended upgrade path, and instead upgrades the firmware directly to the final version. This can result in unexpected configuration loss. To upgrade a device in the GUI, upgrade to each interim version in the upgrade path individually.

For example, when upgrading from 7.0.7 to 7.0.12 the recommended upgrade path is 7.0.7 -> 7.0.9 -> 7.0.11 -> 7.0.12. To ensure that there is no configuration loss, first upgrade to 7.0.9, then 7.0.11, and then 7.0.12.

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

As part of improvements to enhance performance and optimize memory usage on FortiGate models with 2 GB RAM or less, starting from version 7.4.4, FortiOS no longer supports proxy-related features.

This change impacts the FortiGate/FortiWiFi 40F, 50G, 60E, 60F, 80E, and 90E series devices, along with their variants, and the FortiGate-Rugged 60F (2 GB versions only). See Proxy-related features no longer supported on FortiGate 2 GB RAM models for more information.

FortiGate VM memory and upgrade

FortiGate virtual machines (VMs) are not constrained by memory size and will continue to support all available features after upgrading to FortiOS 7.6.0. However, it is recommended to setup VMs with at least 4 GB of RAM for optimal performance.

Managed FortiSwitch do not permit empty passwords for administrator accounts

Starting from FortiOS version 7.4.6, a managed FortiSwitch no longer permits empty passwords for the admin account. If a FortiSwitch unit was previously authorized without an admin password, the FortiGate will automatically generate a random admin password for the FortiSwitch upon upgrading to 7.4.6 or later. This change will cause the admin to lose access.

To regain access, configure a password override on the FortiGate device using the following commands:

```
config switch-controller switch-profile
    edit default
        set login-passwd-override enable
        set login-passwd <passwd>
    next
end
```

FortiSwitch units with an existing admin password will not be affected by this change.

Policies that use an interface show missing or empty values after an upgrade

If local-in policy used an interface in version 7.4.5 GA, or any previous GA version that was part of the SD-WAN zone, these policies will be deleted or show empty values after upgrading to version 7.4.6 or later.

This issue is resolved in FortiOS 7.4.8 with mantis 1104649.

After following the upgrade path to FortiOS 7.4.8, you must manually recreate these policies and assign them to the appropriate SD-WAN zone.

Although not recommended, you can skip the upgrade path and upgrade directly to FortiOS 7.4.8, and the policies remain untouched. Skipping upgrade steps might cause devices to miss other important FortiOS checks and changes and is not recommended.

Statistics for traffic shaping using QTM

Statistics for traffic shaping using QTM, and the `egress-shaping-profile offload` command for SoC5, have been added.

Loopback-based VIPs cannot pass traffic after upgrade

For users upgrading from versions 7.4.5, 7.4.6, and 7.4.7 to version 7.4.8 or later and employing loopback-based VIPs (external IP = loopback IP + `extintf "any"`), the following policy adjustments are recommended to maintain uninterrupted traffic flow if not already configured:

1. Create an entry firewall policy:
   - From external interfaces (for example, `wan1`) to the loopback interface
2. Add an exit firewall policy:
   - From the loopback interface to real-server interfaces (for example, `port4`, `port5`)

FIPS-CC mode no longer supports TACACS+

Starting in FortiOS 7.4.8, TACACS+ is no longer supported in FIPS-CC mode.

Because the TACACS+ protocol is now 30 years old, it uses MD5 for encryption and is insecure. MD5 is not an approved FIPS cipher.

After upgrading to FortiOS 7.4.8 or later, use RADIUS or another authentication method instead of TACAS+. Please note that FortiOS 7.6.0 and later only supports RADIUS over TLS.

30G series upgrade from 7.2.11 to 7.2.12

For the FortiGate and FortiWiFi 30G and 31G devices:

- If trying to upgrade from 7.2.11 GA to 7.2.12 GA directly with BIOS security level High, the upgrade will fail.
- If trying to upgrade from 7.2.11 GA to 7.2.12 GA directly with BIOS security level Low, the upgrade works, but with the following error in the console:

```
****
Fail to append CC_trailer.ncfg_remove_signature:error in stat.
```

```
Fail to ncfg_remove_CC_trailer.
****
```

Product integration and support

The following table lists FortiOS 7.4.9 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 0323 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	• 7.00046
IPS Engine	• 7.00587

See also:

- Virtualization environments on page 27
- Language support on page 27
- SSL VPN support on page 28

- FortiExtender modem firmware compatibility on page 28

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 2019
Windows Hyper-V Server	• Microsoft Hyper-V Server 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

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.

FortiExtender modem firmware compatibility

The following table lists the modem firmware file name and version for each FortiExtender model and its compatible geographical region.

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-101F-AM	FEM_EM06A-22-1-1	FEM_EM06A-22.1.1-build0001.out	America

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEX-101F-EA	FEM_EM06E-22-01-01	FEM_EM06E-22.1.1-build0001.out	EU
	FEM_EM06E-22.2.2	FEM_EM06E-22.2.2-build0002.out	EU
FEX-201E	FEM_06-19-0-0-AMEU	FEM_06-19.0.0-build0000-AMEU.out	America and EU
	FEM_06-19-1-0-AMEU	FEM_06-19.1.0-build0001-AMEU.out	America and EU
	FEM_06-22-1-1-AMEU	FEM_06-22.1.1-build0001-AMEU.out	America and EU
	FEM_06-22-1-2-AMEU	FEM_06-22.1.2-build0001-AMEU.out	America and EU
FEX-201F-AM	FEM_07A-22-1-0-AMERICA	FEM_07A-22.1.0-build0001-AMERICA.out	America
	FEM_07A-22-2-0-AMERICA	FEM_07A-22.2.0-build0002-AMERICA.out	America
FEX-201F-EA	FEM_07E-22-0-0-WRLD	FEM_07E-22.0.0-build0001-WRLD.out	World
	FEM_07E-22-1-1-WRLD	FEM_07E-22.1.1-build0001-WRLD.out	World
FEX-202F-AM	FEM_07A-22-1-0-AMERICA	FEM_07A-22.1.0-build0001-AMERICA.out	America
	FEM_07A-22-2-0-AMERICA	FEM_07A-22.2.0-build0002-AMERICA.out	America
FEX-202F-EA	FEM_07E-22-1-1-WRLD	FEM_07E-22.1.1-build0001-WRLD.out	World
FEX-211E	FEM_12-19-1-0-WRLD	FEM_12-19.1.0-build0001-WRLD.out	World
	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-0-AMEU	FEM_12-22.0.0-build0001-AMEU.out	America and EU
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEV-211F_AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
FEV-211F	FEM_12-22-1-0-AMEU	FEM_12-22.1.0-build0001-AMEU.out	World
FEX-211F-AM	FEM_12_EM7511-22-1-2-AMERICA	FEM_12_EM7511-22.1.2-build0001-AMERICA.out	America
FEX-212F	FEM_12-19-2-0-WRLD	FEM_12-19.2.0-build0002-WRLD.out	World
	FEM_12-22-1-1-WRLD	FEM_12-22.1.1-build0001-WRLD.out	World
FEX-311F	FEM_EM160-22-02-03	FEM_EM160-22.2.3-build0001.out	World
	FEM_EM160-22-1-2	FEM_EM160-22.1.2-build0001.out	World
FEX-511F	FEM_RM502Q-21-2-2	FEM_RM502Q-21.2.2-build0003.out	World
	FEM_RM502Q-22-03-03	FEM_RM502Q-22.3.3-build0004.out	World
	FEM_RM502Q-22-04-04-AU	FEM_RM502Q-22.4.4-build0005_AU.out	Australia
	FEM_RM502Q-22-1-1	FEM_RM502Q-22.1.1-build0001.out	World
	FEM_RM502Q-22-2-2	FEM_RM502Q-22.2.2-build0002.out	World

The modem firmware can also be uploaded manually by downloading the file from the Fortinet Customer Service & Support site. The firmware file names are listed in the third column of the table.

To download the modem firmware:

1. Go to https://support.fortinet.com/Download/FirmwareImages.aspx.
2. From the *Select Product* dropdown, select *FortiExtender*.
3. Select the *Download* tab.
4. Click *MODEM-Firmware*.
5. Select the FortiExtender model and image name, then download the firmware file.

Resolved issues

The following issues have been fixed in version 7.4.9. To inquire about a particular bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
1047112	Performance degradation occurs when IoT database is enabled with Application Control.

DNS Filter

Bug ID	Description
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.
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.

Endpoint Control

Bug ID	Description
1090981	Non-web ZTNA application configurations fail to sync with EMS after initial setup when FortiGate is connected to multiple EMS connectors.
1113593	EMS connector is getting disconnected when using a third-party certificate for verification, resulting in loss of tags and denied traffic.
1142301	ZTNA tag in "View matched endpoint" on GUI might not match backend data.

Explicit Proxy

Bug ID	Description
979401	Cannot choose IPv6 address pool in explicit proxy policy.
1056600	Unexpected behavior occurs during WAD module initialization on FortiGate devices due to improper dependency management leading to order issues or missing dependencies.
1103272	SSL certificates are misapplied when FortiGate processes requests with deny actions in proxy policies.
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.
1166344	WAD session freeze when using explicit proxy with HTTP2 enabled in VDOM UKT-Proxy.
1177548	In session-mode SAML authentication, "400 Bad Request" occurs when accessing CP address.
1178564	Intermittent policy denied issue occurs when explicit proxy policy is configured with SD-WAN zones in outgoing interface.

Firewall

Bug ID	Description
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.
1088905	Virtual server HTTP health-check is always using IP address as a host even when the full URL is configured in http-get.
1116161	Traffic shaping statistics are not provided when using QTM on NP7.
1138259	Traffic breaks when deleting a VLAN interface built upon an NPU VDOM link.
1148166	Source port translation was not permitted with traffic to UDP port 7001.
1159576	Traffic shaping fails when type is set to queuing in the shaping-profile
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.
1186615	When modifying a policy, the "Re-enable filters" option automatically activates, and the policy not being edited is highlighted.

Bug ID	Description
1188448	Traffic drop occurs when configuring virtual wire pair to inspect 802.1Q double tagged VLAN traffic.
1191592	Traffic is misrouted to the FortiGate login page when a VIP with an unresolved FQDN-mapped address is configured.
1025078 1086315	Some customers observed memory usage increase and client session not disconnecting when using virtual server.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1104569	FortiGate FPM hangs after upgrade when confsynchbd fails to release a lock due to file permission issue.
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.
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.
1170088	RADIUS authentication fails when connecting to secondary chassis slots 2 to 4.
1171521	In some cases, after a FortiGate 7000F chassis restart, an FPM may hang while logging in, resulting in the FPM being out of synch with the chassis. This happens because confsynchbd becomes stuck after receiving a management heartbeat from the primary FIM. The issue can occur any time the chassis restarts, including after a firmware upgrade. **Workaround**: The active SMM and the primary FIM must both be in the same slot (for example, FIM1 and SMM1). **1.** Use the SMM `smm_switch` command to change the active SMM. (This may help avoid the issue the next time the chassis restarts.) **2.** Reboot all FPMs. This is not a permanent fix, the issue can occur if the chassis restarts.
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 are not properly inserted as dynamic address objects, causing traffic to fail because traffic could not properly match the related firewall policy.

Bug ID	Description
1181032	Confsync out of sync occurs when configuring an ACME certificate.
1183735	Graceful upgrades lead to unintended primary claiming by FortiGate units during HA resynchronization.

GUI

Bug ID	Description
1040164	Interface X1/X2 does not display on the GUI-Network-Interface page faceplate for FortiGate-90G Gen2.
1112727	Force FortiCare/FortiCloud registration, and only allow exception from a new BIOS setting.
1139922	Cannot rename authorized FortiSwitch.
1145475	Multicast traffic dropped when adding/removing interface bandwidth widget on dashboard.
1146621	When editing an SSL VPN policy in the GUI after creating the policy in the CLI, user/group is not requested.
1149411	Increased Node.js memory usage occurs caused by errorneous memory allocation.
1152464	The DHCP reservation widget incorrectly validates based on the subnet instead of individual IP addresses.
1153415	Multiple GUI errors occur when attempting to view or refresh FMG settings on FortiGate devices managed by FortiManager.
1156109	Console prints error when logging in to the GUI with dns ssl-certificate set to Fortinet_Factory.
1156219	NAC policy deletion fails from the GUI.
1160891	Incorrect inbound traffic values appear on the bandwidth widget for EMAC VLAN interfaces when configured over physical interfaces.
1162818	Proxy policy GUI page keeps loading when using user.certificate in ZTNA proxy-policy.
1170298	Admin timeout occurs when 'admintimeout 0' is set in the admin profile.
1175241	After performing a search in the policy list, sections cannot be collapsed, causing delays in operations.
1177282	Failure to save changes occurs 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.
1198609	Memory usage issues caused by Node.js forking occur when using the JIT optimizer in V8.

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 HA cluster.
1033083	HA sessions are not synchronized properly, causing a high number of sessions on the primary unit, and the standby unit enters into conserve mode.
1068674	PBA logs missing during HA failover.
1133589	HA cluster fails to form when FIPS-CC is enabled.
1143361	Downtime occurs when upgrading HA cluster with HA encryption or authentication enabled.
1148845	LDAP authentication fails when ha-direct is enabled
1151668	Interface bandwidth widget does't display HB and Managed port.
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.
1168328	Mgmt interface is lost when joining a device to a cluster with system dedicated-mgmt enabled.
1170958	HA status shows as 'Unknown' when changing HA group ID.
1171987	HA not synced after modifying one-time 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.
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.
1191128	Intermittent traffic disruption occurs when the secondary FortiGate is rebooting in HA mode.

Hyperscale

Bug ID	Description
1153963	System error when an IPv6 FTP client uses passive mode in NAT64 and the IPv4 FTP server responds with a non-standard response to the PASV command.
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.

Bug ID	Description
1159964	Incorrect duration of hardware sessions occurs when the system is up for a long time.

Intrusion Prevention

Bug ID	Description
1157185	High CPU usage occurs in IPS engine when traffic looping happens due to incorrect VRF validation in local-out path.
1158024	Packet drops and lower CPU utilization on FPC blades when using IPv6 traffic with np-accel-mode enabled and auto-asic-offload.

IPsec VPN

Bug ID	Description
1031789	FortiClient connecting to FGT IPsec VPN with EAP-TTLS authentication does not get TFA push.
1045098	IPv6 traffic is blocked on newly configured IPsec VPN over loopback interface, and reboot needed to fix it.
1057309	Add IPsec SAML external browser support.
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.
1101897	Abnormal spikes in VPN traffic sent bytes occur when counters roll back due to race conditions.
1125487	Gateway switching fails during IKE session resumption when moving from a FortiGate model without Azure AD auto-connect enabled to one with it due to missing mode communication.
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.
1133207	Tunnel establishment fails for multiple FortiGate clients when using DHCP-over-IPSec dial-up VPNs during high concurrent connection attempts.

Bug ID	Description
1137665	OSPF Hello packets cannot be received via VPN after IPsec Rekey when NAT-T is set to 'forced'.
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.
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.
1153984	Authentication error occurs when IPsec-IKEv2 tunnel is configured with FortiToken Cloud.
1162740	Multicast traffic above 1350 bytes does not flow through the IPsec aggregate tunnel when using pre-encapsulation.
1167952	Packets with payload larger than 10K and smaller than 15K are dropped when using IPsec tunnel as egress interface with nTurbo enabled
1169860	L2TPD encountered an internal error.
1172040	Returning packets take a different path when TCP transport is used with multiple default routes in the routing table.
1173228	Default route is added when no IP is available for VPN IPsec RA IKEv2.
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.
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.
1195400	Re-authentication failure occurs when using IPsec IKEv1 after upgrade.
1200669	VPN setting is deleted after device reboot when password policy is enabled and pre-shared key length meets minimum requirements.

Log & Report

Bug ID	Description
998215	Frequent API queries to add and remove objects can result in a memory usage issue on FortiGate.

Bug ID	Description
1005223	Unmatched custom service name appears in traffic log when source port range is defined in custom service
1074236	FGT cannot connect to FortiAnalyzer: hostname resolution failed.
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.
1116428	Observed "Device vulnerability lookup on FortiGuard" under the system event log in high frequency.
1130821	Incomplete log entries occur when attack-context logging is enabled for attacks involving long user-agent strings.
1139748	Different logs appear when unplugging PS1 and PS2 on FortiGate.
1143662	Username truncation occurs in application logs when it exceeds 31 characters
1148101	Logs fail to appear in FortiAnalyzer, and FortiView sources are missing from the Dashboard.
1182491	Traffic logs are not displayed when loading from disk in the FortiGate GUI.
1183091	Security event logs do not load when accessing the 'Security' tab for Forward Traffic.

Proxy

Bug ID	Description
859182	WAD encounters an error condition when configuration changes affect certificate verification processes with Crypto KXP enabled.
1088822	Traffic drop occurs when using proxy-inspection with iOS 18 and HTTP/3 enabled
1107594	Slow website loading occurs when using certificate inspection with proxy inspection-mode in HA Active-Active mode.
1116771	Add a limit on the memory used by user-device-store as a percentage of the total system memory.
1118701	Connection issues for Kentik application using http2 gRPC occur with proxy and deep inspection.
1155858	RD Gateway fails behind HTTPS Virtual Server when using WebSocket upgrade.
1177929	Memory usage issues occur in WAD when handling a large number of sessions.
1183893	Handshake failure occurs when using explicit web proxy with deep inspection to access HTTPS websites through HTTP requests.

REST API

Bug ID	Description
1110811	HTTPSD crash due to a memory leak in the libjson-c library when the monitor/virtual-wan/health-check API returns an error and response is not free correctly.

Routing

Bug ID	Description
969992	FortiGate devices may route SCTP traffic using outdated routes instead of the current optimal path when certain conditions are met.
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.
1134485	Failed to sniff the VNE tunnel interface.
1142290	An error message appears in FortiGate when attempting to add the ssl.root interface to a route-map via the GUI.
1156431	PIM error when receiving PIM Assert with SSM enabled during HA failover.
1171689	Incorrect route selection occurs during BGP redistribution with route maps due to improper handling of parent protocol distances.
1193788	BGP TCP Auth Options key-chain is not applied to the BGP neighbor, causing the neighborship to not establish.

SD-WAN

Bug ID	Description
1130683	Shortcut isn't triggered in certain cases due to the error "found duplicate in ike_check_update_addr_key".

Bug ID	Description
1139734	High latency occurs when a large number of established and monitored shortcuts are present on the FortiGate.
1155927	SD-WAN service events are not logged in SD-WAN events when using SD-WAN rules in standalone mode.
1157493	SD-WAN rule with multiple mac address entries only uses the first mac address when address type is mac.

Security Fabric

Bug ID	Description
1012476	Automation stitches are not synced to downstream FortiGate memory when using CSF external sync API.
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.
1166189	When using the OCI SDN connector, dynamic IP addresses are not fetched correctly if the target compartment contains more than 100 VNICs.
1170605	FortiGate Security Fabric fails to connect with 120G Fabric root.
1174762	Security Ratings incorrectly fail for FortiAP firmware upgrades because the version check does not account for patch numbers.
1180555	Configured IP Address Threat Feed is not connected when pushed via FMG or CLI.

SSL VPN

Bug ID	Description
1026102	SSL VPN encounters a CPU usage issue in the daemon after updating the language from the GUI.
1036557	Performance degradation occurs in SSL VPN due to connection/session timeout management issues.
1042164	Memory usage issues occur when user-peer is used and user login fails in SSL VPN.

Bug ID	Description
1091173	SSL VPN performance drop.
1110039	SSL VPN connection remains active when host-check-interval is set and auth-timeout expires.
1124222	Intermittent connection disruption occurs when using SSL VPN web mode to SSH to Cisco routers with authentication banners.
1126825	SSL VPN stops functioning when ssl.root interface is added to a zone used by at least one policy.
1143541	An error condition occurs in SSL VPN after receiving FortiClient UUID with empty value.
1164811	SSL VPN web mode shows Access Denied error after upgrade on 2GB models.

Switch Controller

Bug ID	Description
961142	An interface in FortiLink is flapping with an MCLAG FortiSwitch using DAC on an OPSFPP-T-05-PAB transceiver.
1064814	Random CPU spikes and for cu_acd process.
1092043	Dynamic VLAN not visible on GUI.
1105000	Aggregate FortiLink went down, and needed to manually down/up the interface.
1114032	The GUI becomes slow or unresponsive when transceiver-related API requests fail.
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.
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.
1146176	config sync error on managed FSW after upgrade when "Name" field and port exported are configured on the same FSW.
1148894	Firmware update status shows as up-to-date for managed FSW when it's actually not on FortiGate.
1149256	Renamed FSW failed to sync to secondary FGT.
1155476	Preconfigure support added for recent FortiSwitch models including FSR-216F-FPOE, FSR-112F-POE, FSR-108F, FS-110G-FPOE, and FS-124G/124G-FPOE.

Bug ID	Description
1155546	Duplicate entries occur in the switch-controller managed-switch list when renaming a managed-switch.
1159594	Verified managed FSW page and related page can load properly.
1173801	High CPU usage occurs when Cu_ACD process is handling FortiSwitch event logs in FortiGate-3501F with large number of switches deployed.
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.
1193309	High CPU usage occurs in cu_acd and fortilinkd processes when managing a large number of FortiSwitches after upgrade.

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.
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.
991285	Broadcasts are unexpectedly forwarded between VxLAN peers when certain FortiGate models are configured as hubs in a Hub-Spoke topology.
992323, 1056133, 1075607, 1082413, 1084898	Traffic interrupt when traffic shaping is enabled on 9xG and 12xG.
999816	FortiGate 100E/101E become unresponsive (No GUI, SSH, console) and requires reboot to regain access.
1046484	After shutting down FortiGate using the "execute shutdown" command, the system automatically boots up again.

Bug ID	Description
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.
1061796	Inaccurate traffic counters display for EMAC-VLAN interfaces when VLAN ID is set to 0 and traffic is offloaded to the NPU.
1064241	FortiGate 100E-series models sometimes become unresponsive.
1065869	SCTP CRC check option is not available on NP7lite platform like 91G/121G.
1084819	FGT80F/81F LACP/shared ports wan1 and wan2 are down after an upgrade or reboot due to hardware shared-port medium changes.
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.
1113436	Packets are dropped when using auto-asic-offload with 802.1AD over LACP on FortiGate due to missing MAC address assignment on QinQ lag interfaces.
1120907	High traffic load on a particular interface causes packet loss on other interfaces of the FortiGate.
1121078	TX Power levels are missing when using FTL4E1QE1CFTN QSFP+ER transceivers on FortiGate devices.
1122446	GPS location updates fail to occur when the GPS signal reception is poor on FortiGate devices.
1130803	Port13-20 speed setting changes to 1000full after FortiGate 10xF reboot.
1140755	When attempting to delete a software switch interface, it becomes permanently hidden due to an unreverted, temporary flag.
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.
1144387	FortiGate 50G DSL fails to acquire an IP address from a DSL modem.
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.
1149508	WAN interface goes down when share-port medium type changes to 'copper' after upgrading FortiGate-80F-DSL
1155410	High memory consumption occurs when node.js encounters catastrophic failures and creates excessive logs.

Bug ID	Description
1156262	An "Input value is invalid." error appears when configuring the maximum number of sessions in FortiGate's global resources.
1156561	NP7lite platforms might encounter high softirq issue and stop processing traffic after running for one month.
1157490	Temperature is out of range with unreasonably high value.
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.
1162489	The SFP WAN1 and WAN2 ports on the FGT-80F device remain down after a reboot when the speed is set to 100M.
1163814	Memory usage issues occur when newcli processes are not deleted after their parent sshd process died.
1164174	Configuration loss occurs when FortiGate enters 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.
1167426	High CPU usage occurs in the linkmtd daemon when large traffic is present.
1168786	100G ports turn up after reboot when administratively down on platforms with Marvell switch like FortiGate 480xF.
1170282	FortiGate HA becomes out of sync after provisioning a certificate by using ACME protocol.
1170291	WWAN interface fails to get IP address when 'auto-connect' feature is enabled.
1172295	Key in router key-chain is not sent in auto-update to FortiManager from FortiGate when creating key-chain and key at the same time.
1173177	High CPU usage occurs when making a configuration change on FortiGate-6301F devices, causing CPU Core0 to spike on all FPC and MBD.
1175221	The 100full speed option is missing for the shared SFP ports of the FortiGateRugged-60F.
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.
1181444	USB-Tethering fails to work on FortiGate 91G when configuring it as a WWAN connection.
1193889	Certificate error occurs when connecting to FAZ via SSH.

Upgrade

Bug ID	Description
1173968	FPMs go to dead state after upgrade.
1196352	FortiExtender configuration is removed after upgrade.

User & Authentication

Bug ID	Description
1017348	Memory usage by fsso_ldap daemon increases continuously when the LDAP server responds with "LDAP_UNWILLING_TO_PERFORM" due to an mishandled memory allocation issue.
1042987	NTLM authentication does not work after upgrade.
1105305	Guest users are not removed after their configured expiry time on certain FortiGate models.
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 becomes unreachable when 'set mfa-mode subject-identity' is configured under the user peer settings, or ha-direct enabled with source-ip.
1146635	Fnband issue during certificate authentication when multiple DNS replies contain both IPv4 and IPv6 parts.
1156903	CLI authentication test fails when RADIUS server has require-message-authenticator setting disabled.
1163152	RADIUS stops working on secondary unit when HA secondary connects to a RADIUS server using UDP.
1177318	Factory default certificates not displaying certificate information in the CLI for FortiGate-201G models.
1193697	Emails with FortiToken codes are not sent due to an SSL error when using SMTPS port 465.

VM

Bug ID	Description
1113362	FGT_VM64_AZURE cannot establish connection with other FGTs in the Security Fabric tree.
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.

Web Filter

Bug ID	Description
1046300	User input ID check doesn't exclude its current-configured ID.
1141367	Intermittent traffic disruption occurs when using Safari browser with proxy-based inspection and certificate inspection enabled.
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.
1177015	Webfilter logs are not generated when https-replacement-message is disabled in proxy-policy with DPI

WiFi Controller

Bug ID	Description
1039985	Erroneous memory allocation observed in the CAPWAP function on NP6 and NP6XLite platforms due to a rare error case.
1147416	Samsung s22 cannot connect WPA3-SAE SSID from local-radio of FWF-70G.
1161023	Groups of WiFi clients are lost after roaming to a different AP, causing unintended behavior in network policies.

Bug ID	Description
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.
1189187	The AP profile's auto-transmit power range adjusts unexpectedly when a single endpoint is modified.

ZTNA

Bug ID	Description
1037749	An error occurs when changing user SAML SP login/logout URL in ZTNA access.
1096134	Failed to apply updated SAML auth configuration after switching IdP from one to another until reboot.
1121978	Adding new HTTPS/HTTP ZTNA server mappings via GUI fails with a duplicate entry error, while attempting to exit after cancellation alters existing entries' URLs.
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.

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 7.4.9.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1183170	SD-WAN is not working in mgmt vdom.

Hyperscale

Bug ID	Description
1027251	Logs are not sent out from FGT with log2host setting when log-server becomes reachable and it has correct dmac.
1034685	Log cache is not cleared and holding the wrong dmac for unreachable gateway.
1042151	syslog over TCP not working.
1058477	sentb and rcvdb show -ve value for end session syslog message.
1069044	Unable to clear/purge npu-session when src filter is set.
1069531	'diag sys session stat' command shows incorrect session_count.
1072076	New HA primary sends syslog session-end log packet using wrong mac address after failover.
1072247	New HA primary does not send syslog session-end log packet after failover.
1078916	Log rate on GUI is double of real log rate.
1085722	Value set for icmpv6-error-rate under sys npu doesn't work.

Bug ID	Description
1091244	'hypersale hw-session-sync-dev' command should print error message when set members over 8.
1091815	Hardware session doesn't sync when one of multiple interface hw-session-sync-dev is down.
1095593	Count for dropping arpmiss exception packets is too high.
1101562	hyperscale hw-session-sync-dev LAG members can exceed 2*number of NP.
1119021	Sessionsync daemon makes hw-session-sync dev up even it's physically down, no such issue with sw session sync dev.
1119031	HW sessions are not synced to secondary when one of the hw-session-sync-dev members is down.
1128155	FGT 1801F log-transport TCP should be hidden for log servers under L2host and Netflow on CLI.
1135433	IPv6 entries appear in the output of pba list after reaching max PBA limit for ippool.
1138823	FGT1801F non-hyperscale VDOM shows incorrect output of 'diag firewall ippool get-pub/priv' commands.
1140493	Config should be blocked when user tries to set same interface as hw-session-sync-dev andmonitor.
1141632	After HA failover, syslog packets not sent out from new HA primary when using NAT46/NAT64 policies.
1143144	Both `HW log(ps) rate` and `log(pm) rate` show in `dia sys npu-session stat`when `set log-mode per-nat-mapping` is enabled.
1144290	Log rate shows 0 when using TCP for syslog.
1150863	Session deleted after FGSP failover due to dirty r-session.
1184045	v6 TCP/UDP traffic doesn't pass when threatfeed object is used in v6 HS policy.
1197891	When unsupported ports are configured for hw-session-sync-dev, it results in hardware session sync not functioning correctly. **workaround**: Change interface and reboot because fixing the config does not restore the proper configuration.
1199557	Unsupported ports allowed to be configured as part of the lag for hw-session-sync-dev.
1200885	Renaming ippool causes "NPD-0 :PRP ADD FAIL!" error.
1201968	Memory leak/ leak to log2host tbl can be seen when there are ~60M cc with log2host setting after couple of failovers.
1202268	Not all the HW sessions are synced to new secondary after a failover.
1203844	Upgrade: cgn-log-server-grp config is missing after upgrade from 7.2.12 to 7.4.9.

System

Bug ID	Description
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'.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.4.9.

Explicit Proxy

Bug ID	Description
1026362	Web pages do not load when `persistent-cookie` is disabled for `session-cookie-based authentication` with *captive-portal*.

Firewall

Bug ID	Description
959065	On the *Policy & Objects* > *Traffic Shaping* page, when deleting or creating a shaper, the counters for the other shapers are cleared.
1114635	Unable to filter address object by CIDR notation.

FortiGate 6000 and 7000 platforms

Bug ID	Description
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.
1006759	After an HA failover, there is no IPsec route in the kernel. **Workaround**: Bring down and bring up the tunnel.
1026665	On the FortiGate 7000F platform with virtual clustering enabled and syslog logging configured, when running the `diagnose log test` command from a primary vcluster VDOM, some FPMs may not send log messages to the configured syslog servers.

Bug ID	Description
1048808	If the secondary reboots, after it rejoins the cluster SIP sessions are not resynchronized.
1070365	FGCP HA session synchronization may stop working as expected on a FortiGate 7000F cluster managed by FortiManager. This happens if the HA configuration uses management interfaces as session synchronization interfaces by configuring the `session-sync-dev` option, for example: config system ha set session-sync-dev 1-M1 1-M2 end The problem occurs when FortiManager updates the configuration of the FortiGate 7000F devices in the cluster it incorrectly changes to the VDOM of the management interfaces added to the `session-sync-dev` command from `mgmt-vdom` to `vsys_ha` and the interfaces stop working as session sync interfaces. You can work around the problem by re-configuring the `session-sync-dev` option on the FortiGate 7000F cluster (this resets the VDOM of the session sync interfaces to `vsys_ha`) and then retrieving the FortiGate configuration from FortiManager. This synchronizes the correct configuration to FortiManager.
1078532	When upgrading the FG6001F platform, in some instances, the slave chassis does not synchronize the FPC subscription license from master chassis. **Workaround**: use the `execute update-now` command.
1092728	On FortiGate 6000 and 7000 platforms, fragmented IPv6 traffic is randomly dropped.
1153360	Counter values fail to match totals and may overflow during continuous clearing in certain FortiGate models.
1185528	Subscription license on the secondary chassis is missing after the graceful upgrade from 7.2.10/11 to 7.2.12. **Workaround**: run `execute update-now` again.

FortiView

Bug ID	Description
1123502	FortiView Threats: drill down to malicious website entry, and *Failed to retrieve FortiView data from disk* is returned.

GUI

Bug ID	Description
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 100000 entries.
885427	Suggest showing the SFP status information on the faceplate of FGR-60F/60F-3G4G devices.

Bug ID	Description
1024000	FGT 4400F displays TB on 2 x 100 Gig VLAN interface bandwidth widget.
1071907	There is no setting for the type option on the GUI for npu_vlink interface.
1145907	Bandwidth widget does not report the traffic correctly for backup VLAN interfaces.
1153294	Custom HTML content does not render correctly on login pages when configured through the FortiGate web interface or CLI.

HA

Bug ID	Description
781171	When performing HA upgrade in the GUI, if the secondary unit takes several minutes to boot up, the GUI may show a misleading error message *Image upgrade failed* due to premature timeout. This is just a GUI display issue and the HA upgrade can still complete without issue.

Hyperscale

Bug ID	Description
817562	lpmd fails to correctly handle different VRFs, treating all as vrf 0, causing improper route management and affecting network traffic isolation.
896203	NPD parse errors occur after system reboot when running with multiple VDOMs and large address groups.
961328	Port selection remains in direct mode despite setting pba-port-select-mode to random, causing non-random port allocation for NAT sessions.
977376	FG-4201F has a 10% performance drop during a CPS test case with DoS policy.
1025908	Session count on peer device is 50% less during fgsp testing in new setups using VRRP-based configuration.

IPsec VPN

Bug ID	Description
866413	Traffic over GRE tunnel over IPsec tunnel, or traffic over IPsec tunnel with GRE encapsulation is not offloaded on NP7-based units.
897871	GRE over IPsec does not work in transport mode.
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.

Bug ID	Description
970703	FortiGate 6K and 7K models do not support IPsec VPN over vdom-link/npu-vlink.
1125487	Autoconnect to IPsec VPN using Entra ID logon fails when there are multiple IPsec tunnels.

Proxy

Bug ID	Description
910678	CPU usage issue in WAD caused by a high number of devices being detected by the device detection feature.
1035490	The firewall policy works with proxy-based inspection mode on FortiGate models with 2GB RAM after an upgrade. *Workaround*: After an upgrade, reboot the FortiGate.

REST API

Bug ID	Description
1154124	FortiNAC dynamic address REST API request through FortiGate Security Fabric denied with HTTP 400 Bad Request.

Routing

Bug ID	Description
903444	The `diagnose ip rtcache list` command is no longer supported in the FortiOS 4.19 kernel.

1040655	From version 7.4.1, when there is ECMP routes, local out traffic may use a different route/port to connect out to the server.
	Workaround: for critical traffic which is sensitive to source IP address, specify the interface or SD-WAN for the traffic using the `interface-select-method` command for nearly all local-out traffic. For example:
	`config system fortiguard`
	`  set interface-select-method specify`
	`  set interface "wan1"`
	`end`

1133796	IPv6 routes are stuck on kernel routing table.
1150878	The IPoE tunnel interface cannot be selected in the Interface Bandwidth widget.

Security Fabric

Bug ID	Description
1076439	Security Fabric Asset Identity Center shows *"Failed to load user device store data"*.
1154494	Automation stitch for non-root FGT in Security Fabric is not triggered.
1156006	SFTP backup fails to execute as expected when triggered through the automation stitch.

Switch Controller

Bug ID	Description
1150215	Offline FSWs show as offline in the GUI topology view but show as online in the list view.
1153175	Intermittent issues configuring allowed VLANs on the MCLAG interface using FortiGate GUI and CLI.
1153905	FortiSwitch client page keeps loading.

System

Bug ID	Description
912383	FGR-70F and FGR-70F-3G4G failed to perform regular reboot process (using `execute reboot` command) with an SD card inserted.
995011	FG-4201F NP7 HPE showed all-protocol packets dropped, even though `all-protocol` had been disabled by setting it to `0`.
1021903	The le-switch member list does not update when the role of an interface is changed in a lan-extension environment.
1078541	The FortiFirewall 2600F model may become stuck after a fresh image burn. Upgrading from a previous version stills works. **Workaround**: power cycle the unit.
1085407	FortiGate unresponsive when `default-qos-type` is set to `shaping`.
1105321	FG-4201F with NP7 network processors shows EIF0_IGR and EIF1_IGR usage stuck at 100% and host softirq stuck at 99% after running the iptunnel traffic.
1114298	FortiGate Cloud remote login triggers two admin login events (1 successful and 1 unsuccessful for PKI admin).
1136616	No graphs on some VLAN interfaces in dashboard Interface widget.
1164332	NP7 stops forwarding traffic after reassembling large packet in DFR.

Upgrade

Bug ID	Description
1114550	FortiExtender shows as offline after upgrading FGT from 7.4.5 to 7.4.6. **Workaround**: Reboot FortiExtender manually.

User & Authentication

Bug ID	Description
884462	NTLM authentication does not work with Chrome.
972391	RADIUS group usage not displayed correctly in GUI when used for firewall admin authentication.
1082800	When performing LDAP user searches from the GUI against LDAP servers with a large number of users (more than 100000), FortiGate may experience a performance issue and not operate as expected due to the HTTPSD process consuming too much memory. User may need to stop the HTTPSD process or perform a reboot to recover. **Workaround**: Perform an LDAP user search using the CLI.
1148767	FSSO users are showing in small letters, filtering of users is not working, and PIE charts are also not visible.

VM

Bug ID	Description
978021	In FTP passive mode with GWLB setup, Geneve header VNI lengths are zero in syn-ack packets, leading to retransmission issues.
1125437	The "set distance" option under interface configured as dhcp client doesn't work on VM.
1172881	IPS engine crash w DPDK enabled, stress traffic over ipsec tunnel and fragmentation, and "system affinity-packet-redistribution".

WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the *Managed FortiAPs* page and *FortiAP Status* widget can take a long time to load. This issue does not impact FortiAP operation.

Bug ID	Description
964757	The FortiGate fails to generate debug/sniffer logs for a user when connecting to a specific SSID despite showing station logs with radius requests and challenges, while other SSIDs function correctly.
972093	RADIUS accounting data usage is different between the bridge and tunnel VAP.
1080094	Offline station data consumes excessive memory when the `sta-offline-cleanup` or `max-sta-offline` settings are not configured.
1144969	Mismatch IP address details in *WiFi Client* GUI page.

ZTNA

Bug ID	Description
819987	Mapped drives become inaccessible after laptop reboots when using FortiGate ZTNA access proxy with FQDN destinations.

Built-in AV Engine

AV Engine 7.00046 is released as the built-in AV Engine.

Built-in IPS Engine

IPS Engine 7.00587 is released as the built-in IPS Engine.

Resolved engine issues

Bug ID	Description
1108944	DNS translation on FortiGate strips out CNAME when doing translation.
1159485	Traffic is multiplicated when SSL deep inspection is used with DPDK enabled/disabled.
1168879	Dynamic content of webpages does not loaded correctly.
1184183	Accessing a URL one time results in two reduplicative logs being recorded in the webfilter log.

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.

Limitations on HA cluster formation between different FortiGate Rugged 60F and 60F 3G4G models

FortiGate Rugged 60F and 60F 3G4G models have various generations defined as follows:

- Gen1
- Gen2 = Gen1 + TPM
- Gen3 = Gen2 + Dual DC-input
- Gen4 = Gen3 + GPS antenna
- Gen5 = Gen4 + memory

The following HA clusters can be formed:

- Gen1 and Gen2 can form an HA cluster.
- Gen4 and Gen5 can form an HA cluster.

- Gen1 and Gen2 cannot form an HA cluster with Gen3, Gen4, or Gen5 due to differences in the `config system vin-alarm` command.

www.fortinet.com