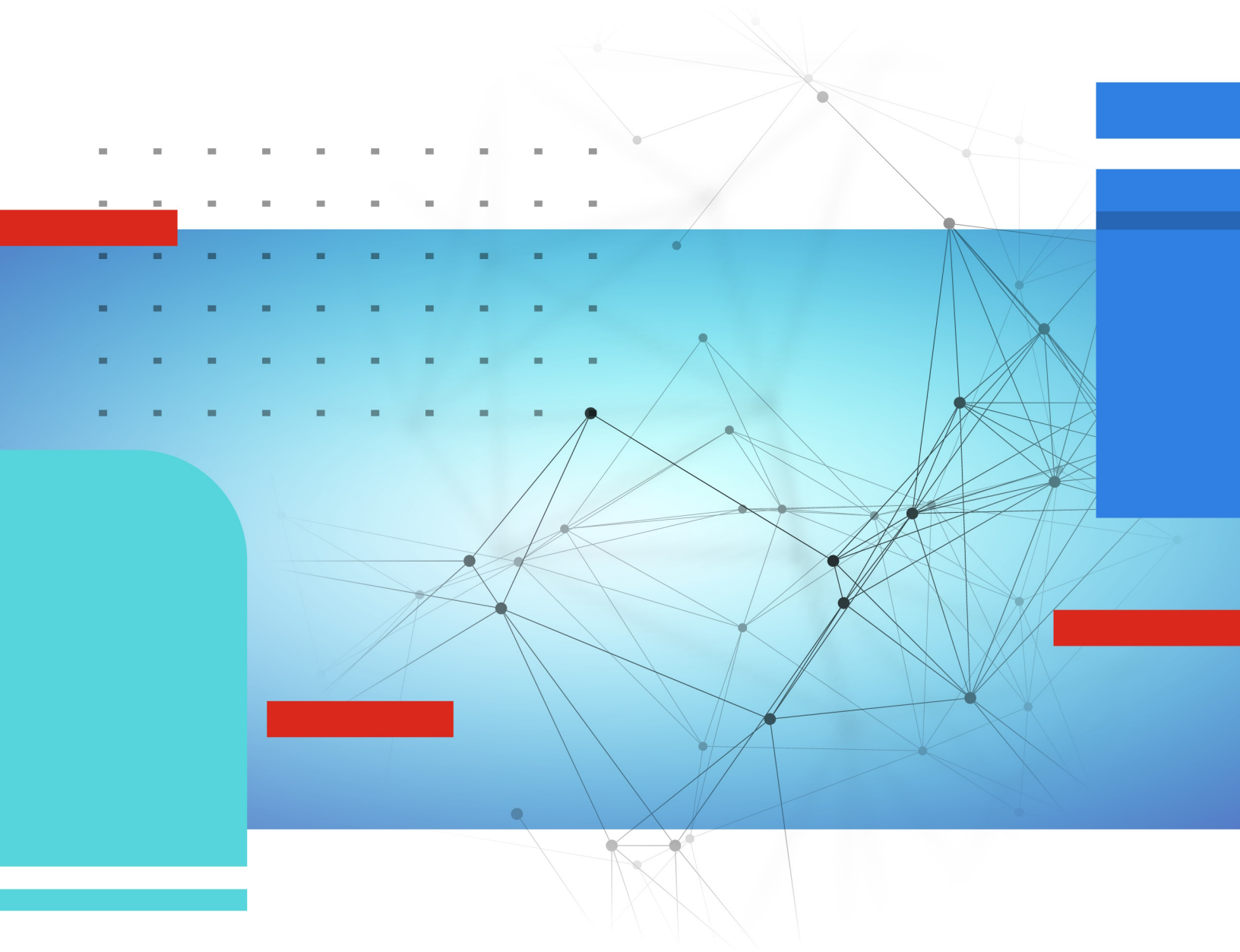
Release Notes

FortiOS 7.6.4



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

August 21, 2025
FortiOS 7.6.4 Release Notes
01-764-1174535-20250821

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-08-21	Initial release.
2025-08-21	Added Changes in default behavior on page 16 and Changes in table size on page 18. Updated Special notices on page 9, Upgrade information on page 25, Resolved issues on page 36, and Built-in IPS Engine on page 61.

Introduction and supported models

This guide provides release information for FortiOS 7.6.4 build 3596.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.6.4 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-50G, FG-50G-5G, FG-50G-SFP, FG-50G-DSL, FG-50G-SFP-POE, FG-51G, FG-51G-5G, FG-51G-SFP-POE, FG-60F, FG-61F, FG-70F, FG-70G, FG-70G-POE, FG-71F, FG-71G, 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-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-SFP, FWF-50G-DSL, FWF-51G, FWF-60F, FWF-61F, FWF-70G, FWF-70G-POE, FWF-71G, 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-70G, FGR-70G-5G-Dual, FGR-70F-3G4G
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 7.6.4 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

FortiGate cannot restore configuration file after private-data-encryption is re-enabled

In a new enhancement, enabling `private-data-encryption` will utilize a randomly generated private key. Therefore, FortiGate cannot restore the configuration file in the following sequence:

1. `private-data-encryption` enabled with random key, and configuration is backed up.
2. `private-data-encryption` disabled.
3. `private-data-encryption` enabled again, with new random key.
4. Restore configuration file in step 1.

When disabling `private-data-encryption`, a warning in the CLI will be displayed:

```
This operation will restore system default data encryption key!
```

```
Previous config files encrypted with the private key cannot be restored after this operation!
```

```
Do you want to continue? (y/n)y
```

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 7.6.3 and later 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 7.6.3 can centrally manage FortiGates with the private-data-encryption setting enabled, with the following limitations:

- FortiManager cannot import objects that include the password type attribute.
- 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.

FortiOS upgrade behavior with FortiManager 7.6.2 and earlier

If in FortiOS 7.4.5 or 7.6.0 the 32-digit hexadecimal private key is enabled, and then the FortiGate device is upgraded to 7.6.1, the 32-digit hexadecimal `private-data-encryption` key is preserved. As a result, FortiManager 7.6.2 and earlier is aware of the 32-digit hexadecimal `private-data-encryption` key and can continue to manage the FortiGate device. However, if the `private-data-encryption` key is enabled after an upgrade of FortiOS to 7.6.1, FortiManager 7.6.2 and earlier no longer can manage FortiGate devices running FortiOS 7.6.1.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.6.4 features.

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`).

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.6.4 features.

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

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.

RADIUS vulnerability

Fortinet has resolved a RADIUS vulnerability described in CVE-2024-3596. As a result, firewall authentication, FortiGate administrative GUI authentication, and WiFi authentication may be affected depending on the functionality of the RADIUS server software used in your environment. RFC 3579 contains information on the affected RADIUS attribute, message-authenticator.

In order to protect against the RADIUS vulnerability described in CVE-2024-3596, as a RADIUS client, FortiGate will:

1. Force the validation of message-authenticator.
2. Reject RADIUS responses with unrecognized proxy-state attribute.

Message-authenticator checking is made mandatory under UDP/TCP. It is not mandatory when using TLS. Therefore, if FortiGate is using UDP/TCP mode without RADSEC, the RADIUS server should be patched to ensure the message-authenticator attribute is used in its RADIUS messages.

Affected Product Integration

- FortiAuthenticator version 6.6.1 and older
- Third party RADIUS server that does not support sending the message-authenticator attribute

Solution

- Upgrade FortiAuthenticator to version 6.6.2, 6.5.6 or 6.4.10 and follow the upgrade instructions: https://docs.fortinet.com/document/fortiauthenticator/6.6.2/release-notes/859240/upgrade-instructions
- Upgrade the RADIUS server and/or enable it to send the correct message-authenticator attribute

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.

SSL VPN tunnel mode replaced with IPsec VPN

Starting in FortiOS 7.6.3, the SSL VPN tunnel mode feature is replaced with IPsec VPN, which can be configured to use TCP port 443. SSL VPN tunnel mode is no longer available in the GUI and CLI. Settings will not be upgraded from previous versions. This applies to all FortiGate models.

To ensure uninterrupted remote access, customers must migrate their SSL VPN tunnel mode configuration to IPsec VPN before upgrading to FortiOS 7.6.3 and later.

See Migration from SSL VPN tunnel mode to IPsec VPN in the *FortiOS 7.6 New Feature*guide for detailed steps on migrating to IPsec VPN before upgrade.

A complete migration guide can be found in the following links:

- For FortiOS 7.6, see SSL VPN to IPsec VPN Migration.
- For FortiOS 7.4, see SSL VPN to IPsec VPN Migration.

Agentless VPN (formerly SSL VPN web mode) not supported on FortiGate 40F, 60F, and 90G 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-60F/FWF-60F
- FGT-61F/FWF-61F
- FGR-60F and variants (2GB versions only)
- 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 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 proxy-related features.

This change impacts the FortiGate 40F and 60F 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.

GUI access conflict with IPSec TCP tunnel on the same interface

In FortiOS version 7.6.1, the default IKE TCP port has been changed to port 443 on new deployments. In the FortiOS 7.6.1 Release Notes, see Bug ID 1051144 in Changes in default values.

This may affect GUI access for interfaces bound to an IPsec tunnel in the scenario that the GUI admin port is also using port 443.

In case GUI connectivity is lost, connect to the FortiGate by:

1. Connecting from an interface that is not bound to an IPsec tunnel.
2. Connecting to the interface using SSH, if SSH is enabled.
3. Connecting to the FortiGate from console.

To ensure continued functionality, users are recommended to either:

- Choose an alternative interface for GUI access by configuring:

```
config system global
    set admin-sport <port>
end
```

- Customize the `ike-tcp-port` to a value other than 443:

```
config system settings
    set ike-tcp-port <port>
end
```

Changes in default behavior

Bug ID	Description
1099339	The IPv4 address field for VNE interfaces enforces a /32 netmask. This change requires manually adding a route to the interface on the peer side of the VNE tunnel to reach it.

Changes in default values

Bug ID	Description
1109950	The default value for `svr-pool-multiplex` under `config firewall access-proxy` has been changed from `enabled` to `disabled`. This setting controls whether server pool multiplexing is used to share connected servers across HTTP, HTTPS, and web portal API gateway sessions.

Changes in table size

Bug ID	Description
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.

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.

LAN Edge

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

Feature ID	Description
656793	Support for storm-control burst size level has been added to the FortiSwitch controller, enabling configuration at the global level, for each managed switch, and for each port within storm control policies. This enhancement allows users to control the maximum number of packets or bytes permitted when storm control is activated.

673599	Add support for IP source guard event logging on the switch-controller. This enhancement introduces new CLI commands to enable log violations and configure a violation timer, enhancing network security monitoring capabilities.
	
	`config switch-controller ip-source-guard-log`
	`  set log-violations { enable | disable}`
	`  set violation-timer`
	`end`

945633	You can now use both FortiSwitch network access control (NAC) and 802.1X authentication on the same switch port. After a device is successfully authenticated with 802.1X authentication, the NAC user policy checks if the device is assigned to a specific user group. If the device matches the NAC user policy, it is assigned to a specific VLAN.

Feature ID	Description
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.
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.

Log & Report

See Logging in the New Features Guide for more information.

Feature ID	Description

1113685	With the new `srczone` and `dstzone` fields, users can now search logs by zone names, enhancing scalability and efficiency in log management. Previously, searches had to be done by individual interfaces within zones.
	
	`config log setting`
	`  set zone-name {enable | disable}`
	`end`

Network

See Network in the New Features Guide for more information.

Feature ID	Description
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 the user experience.
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.

Policy & Objects

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

Feature ID	Description
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.
1132012	Filtering support has been added to multiple 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.
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 agent's 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.

SD-WAN

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

Feature ID	Description
1135778	Previously when using load-balance SLA service, SD-WAN attempts to build all possible shortcuts using all overlay (VPN) paths between spokes. This brings no value for shortcuts that share the same underlay (source and destination interface IP addresses). This new feature ensures that all created shortcuts use unique underlay paths. Once shortcuts are created on all distinct underlay paths, user traffic is load-balanced between in-SLA shortcuts, rather than between in-SLA shortcuts and parents.
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.
1158785	The feature enables a new hybrid mode where SLA mode and Priority mode work together for sla-mode service rule. In this mode, SD-WAN selects the best member based on both SLA value and link quality (for example, latency/jitter/packet-loss). In addition, health-check is extended to support "custom-profile" as link-cost-factor, allowing for a more customized SLA evaluation based on various link quality metrics.

Feature ID	Description
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.

Security Profiles

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

Feature ID	Description
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.
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.
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 streamline security operations.

System

See System in the New Features Guide for more information.

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.
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.
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 Support (EOS) 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.

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 interfacesincluding members of aggregate interfacesare 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`

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 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.

WiFi Controller

See Wireless in the New Features Guide for more information.

Feature ID	Description
1107133	Support for zero-touch provisioning (ZTP) has been implemented, allowing mesh leaf FAPs to automatically detect the FortiGate via the default mesh link using predefined mesh settings. This eliminates the need for users to manually log in to each leaf FAP, significantly reducing the time and effort required for configuring mesh networks, thereby enhancing efficiency and improving the user experience.

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`

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.

ZTNA

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

Feature ID	Description

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.

1135779	In this enhancement, new ZTNA error codes 024 and 025 are added as well as improvements to certain ZTNA replacement messages with error codes 064 and 065.

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 25 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 7.6.4 is verified to work with these Fortinet products. This includes:

FortiAnalyzer	• 7.6.4
FortiManager	• 7.6.4
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 7.6.0, use FortiClient 7.6.0.

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 7.6.4. When Security Fabric is enabled in FortiOS 7.6.4, all FortiGate devices must be running FortiOS 7.6.4.

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 7.6.4:

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 7.6.4 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.

Default setting of cp-accel-mode is changed to none on 2GB memory models

This change disables CP acceleration to lower system memory usage thus can prevent some unexpected behavior due to lack of memory.

Previous FortiOS CLI behavior:

```
config ips global
    set cp-accel-mode advanced
end
```

New FortiOS CLI behavior after upgrade:

```
config ips global
    set cp-accel-mode none
end
```

This change will cause performance impact as CPU will do the pre-match (pattern match) inside IPS (CPU) instead of hardware engine (cp module in SOC4). Some customers could expect an increase in CPU utilization as a result.

FortiGate and FortiWiFi 4xF/6xF families are affected by this change.

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

If local-in policy, DoS policy, interface policy, multicast policy, TTL policy, or central SNAT map used an interface in version 7.4.5, 7.6.0 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 7.6.1 or later.

This issue is resolved in FortiOS 7.6.3 with mantis 1104649.

After following the upgrade path to FortiOS 7.6.3, 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 7.6.3, and the policies remain untouched. Skipping upgrade steps might cause devices to miss other important FortiOS checks and changes and is not recommended.

Managed FortiSwitch do not permit empty passwords for administrator accounts

Starting from FortiOS version 7.6.1, 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 7.6.1 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.

Removed speed setting affects SFP+ interfaces after upgrade

Starting in FortiOS 7.6.1, the `1000auto` speed setting is removed. If a FortiGate SFP+ port speed is set to `1000auto` before upgrade, the upgrade process automatically changes the setting to `10000full`. This change can cause the interface to go down when the connecting device has a different speed setting.

Workaround: After upgrade, align the port settings. Edit the port and set the speed to `1000full` to restore the connection.

```
config system interface
    edit <port>
        set speed 1000full
    next
end
```

Hyperscale with FGCP HA clusters and interface monitoring

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 or later, 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.

Product integration and support

The following table lists FortiOS 7.6.4 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	• 7.01154

See also:

- Virtualization environments on page 32
- Language support on page 32
- Agentless VPN support on page 33

- FortiExtender modem firmware compatibility on page 33

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, 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	✓

Agentless VPN support

The following table lists the operating systems and web browsers supported by Agentless VPN (formerly SSL VPN web mode). See also SSL VPN tunnel mode replaced with IPsec VPN on page 13.

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
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

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
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
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

FortiExtender model	Modem firmware image name	Modem firmware file on Support site	Geographical region
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 7.6.4. To inquire about a particular bug, please contact Customer Service & Support.

Agentless VPN (formerly SSL VPN web mode)

See also SSL VPN tunnel mode replaced with IPsec VPN on page 13.

Bug ID	Description
1115577	Add customization support for the SSL-VPN header replacement message.
1134189	Connection refused occurs when using custom landing page in agentless VPN portal on FortiGate.
1143541	An error condition occurs in sslvpn after receiving FortiClient UUID with an empty value.

Anti Spam

Bug ID	Description
1098623	A closing character ">" of HTML tag is missing in replacement message of antispam URL spam submission text when FortiGate processes spam emails.

Anti Virus

Bug ID	Description
1080003	FGT memory gradually increases when FGT Flow AV Profile is inspecting TCP 6200 traffic with outbreak prevention enabled.

Application Control

Bug ID	Description
1118703	Web traffic designated as blocked is allowed due to the config entry priority in the application control profile.
1136103	App categories fail to display in NGFW mode due to undefined object causing JavaScript TypeError during app category data access.

DNS Filter

Bug ID	Description
1134108	The IPS engine memory usage increases rapidly when a flow-based policy uses an external Threat Feed with over 1M domain entries, causing device unresponsiveness.
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.

Endpoint Control

Bug ID	Description
1142301	ZTNA tag in "View matched endpoint" on GUI might not match backend data.

Explicit Proxy

Bug ID	Description
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.
1096263	Intermittent 504 errors occur when an IPv6 HTTP request followed by an IPv4 request in the same pipeline goes through explicit proxy with outgoing-ip.

Bug ID	Description
1116834	Authentication pop-up does not appear when accessing HTTPS websites through FortiGate with Explicit Proxy when authentication rules, webproxy-forward-server, and certificate-inspection are configured in proxy-policy.
1136596	Incorrect status display occurs when editing proxy policies for hard/software switches on some FortiGate models.
1139784	Machine account is treated as NULL user in Kerberos and fails to authenticate via Kerberos.
1144818	Download failure occurs when accessing https://7-zip.de for domain objects.githubusercontent.com.

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.
1057080	On the Firewall Policy page, search results do not display in an expanded format.
1108236	Incorrect logs are displayed when viewing matching logs for an implicit deny policy due to an invalid filter operator.
1114635	Not able to filter address object by CIDR notation.
1131860	A two to three minute delay occurs when enforcing policy changes to existing or new traffic due to linear duplicate address checks during iprope updates.
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.
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.
1155687	DNAT incorrect in later FTP data packets, and FTP data session gets reset when FTP server responds with public IP in PASV mode.
1158137	Traffic is blocked when UTM and Nturbo are enabled in firewall policy for np7lite platforms.
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.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1014826	SLBC does not function as expected with IPsec over TCP enabled.
1060864	Ports fail to establish or exhibit CRC/input errors when 100G QSFP28 LR transceivers are used with FIM-7920E and Cisco ASR in specific setups.
1103810	100G SFPs are experiencing compatibility issues with the 7060E at Turkcell.
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.
1131541	SSL VPN load balance settings remain active in FortiOS configurations where SSL VPN tunnel mode has been removed.
1135891	The PSU status incorrectly shows as "Critically High" on the GUI dashboard widget.
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.
1153360	Counter values fail to match totals and may overflow during continuous clearing in certain FortiGate models.
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.
1170210	FGT Wireless controller Wifi client cannot ping GW/FGT interface. Pass through traffic works fine.
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.
1172922	SDN dynamic address synchronization flaps or fails when SDN connectors are frequently enabled and disabled.
1183735	Graceful upgrade from 7.2.10/11 to 7.4.9 build 2812 fails because HA secondary cannot take HA primary.

FortiView

Bug ID	Description
1133164	Subnet filtering fails for firewall users due to partial API support.
1138980	Read-only profile admin user tries to change FortiView source time range , and it is logged as edit by 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.

GUI

Bug ID	Description
264694	When a firewall user logs in via the GUI using RADIUS with FortiToken, no accounting request is generated.
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.
1126162	Hostname pop-up window shows "failed to retrieve info" error in *System* > *HA* page.
1129254	Unexpected behavior occurs when attempting to save L2TP dialup tunnel configurations using SD-WAN members on some FortiGate models.
1130636	The FortiConverter window reappears after closing even when *Don't show again* is selected.
1131500	Some bandwidth interface widget not show historical information.
1137821	Failed to open CLI console from downstream FGT GUI with error "Connection lost." with SAML SSO admin login.
1138359	Can't open CLI console when logging in with SSO account.
1139922	Cannot rename authorized FortiSwitch.
1140317	FAP/FSW registration status appears vacant on Firmware & Registration page.
1143611	User/groups objects disappear after editing firewall policy.
1145475	Multicast traffic dropped when add/remove 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.

Bug ID	Description
1148930	Exported FSW 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.
1150591	Node.js encounters an error when attempting to read the property from a null value, causing unintended behavior on some FortiGate models.
1151414	Unable to connect to FortiSwitch CLI via Diagnostics and Tools.
1152464	DHCP reservation from DHCP monitor page checks DHCP IP range instead of subnet/netmask.
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.

HA

Bug ID	Description
794395	The secondary unit in an HA cluster would display messages indicating that external resources were not in sync, despite the resources being correctly synchronized.
1017177	A WAD processing issue causes the SNMP to not respond in a HA cluster.
1080655	HA synchronization fails after configuration changes on FortiGate devices due to improper handling of a hasync flag in the fgfmd daemon.
1126274	VDOM is created unexpectedly when changing VRRP priorities on multiple interfaces if standalone-config-sync is enabled.
1133589	HA cluster fails to form when FIPS-CC is enabled.
1135008	When link monitor fail, initial HA cluster failover doesn't happen immediately until pingserver-flip-timeout expires.
1136097	HA state may become out of sync due to a race condition caused by missing local-in ipropes.
1141528	High CPU usage occurs when FortiGate secondary unit is started in Azure vWAN SD-WAN NGFW with Dynamic rerouting.
1143361	Downtime occurs when upgrading HA cluster with HA encryption or authentication enabled.
1143791	The heartbeat interface default route is lost and HA fails to sync when changing the interface mtu-override option.
1151668	Interface bandwidth widget doesn't display HB and Managed port.
1162432	Split brain occurs when renaming IPsec phase1-interface in a with a lot of VDOMs.

Bug ID	Description
1172590	An error condition occurs in FortiGate when running the `diag sys ha nonhaconf` command on the secondary node in an HA cluster.
1179351	FortiGate failed to load the private keys for factory certificates to fgfmd due to incorrect classification

Hyperscale

Bug ID	Description
1089281	With FG-480xF/FFW-480xF using npu-group other than "0" with log2host with around ~1M CPS could result in NP chip getting stuck.
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.

Intrusion Prevention

Bug ID	Description
1117043	Fatal errors occur when the IPS engine sends requests with zero-length data segments to IPSA. This issue only affects physical FortiGate models with the following IPS engine versions: • IPS Engine version: 7.550 - 7.567 • IPS Engine version: 7.1019 - 7.1039 To determine the IPS Engine versions, use the command: `get sys fortiguard-service status | grep 'IPS/FlowAV Engine'`
1122188	Internal diagnostic commands fail or delay when ipsmonitor processes each request sequentially due to sequential forwarding to IPS daemon processes.
1149760	Inline-IPS fails to match sensor locations for the "Web.Server.Password.File.Access" signature because it incorrectly reverses traffic direction definitions.

IPsec VPN

Bug ID	Description
979591	Changes to IPsec phase1 fragmentation settings do not take effect immediately when made on dynamic configurations.
995912	VPN tunnels exhibit instability following an upgrade, with processes stuck during NP7 debugging due to improper prioritization of certain packets.
1063528	Incorrect MTU settings prevent fragmented packets from being properly offloaded in IPsec tunnels, causing high CPU usage on FortiGate models.
1068626	SOC4 platform IPsec traffic is unexpectedly stopped because of IPsec outbound hung.
1101897	Abnormal spikes in VPN traffic sent bytes occur when counters roll back due to race conditions.
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.
1135490	Static route towards remote side of IPsec tunnel becomes inactive when tunnel IP address is configured.
1140823	IPsec tunnels become stuck on spoke np6xlite, causing ESP packet drops after extended operation due to improper vifid formation during multiple rekey operations.
1145219	IPsec tunnels drop unexpectedly during rekeying when using certificate authentication with multiple dialup gateways and peer-initiated SA_INIT requests.
1145391	IPsec VPN tunnel fails to establish when QKD is required.
1145411	Changing the ip-fragmentation setting on dynamic IPsec phase1 does not take effect immediately after modification due to an issue with the change handler function in certain FortiOS builds.
1147023	VPN traffic halts unexpectedly on the spoke when FEC is disabled during connection cleanup after failed phase 1 negotiations, affecting dynamic tunnel handling.
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.
1162270	Secondary IPsec tunnel cannot come up after primary tunnel is down and config change when "set monitor" is configured under phase1.

Log & 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.
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.
1116108	Intra-zone Local logs are missing when intrazone allow is enabled.
1141436	FortiGate device enabled with FIPS-CC mode sends an incorrect build number (0523) to FortiGate Cloud.
1141733	Traffic interruptions occur when revisiting the forward traffic log page during searches with applied filters.
1142836	Broadcast traffic is logged when `local-in-deny-broadcast` setting is disabled.
1148101	Logs fail to appear in FortiAnalyzer, and FortiView sources are missing from the Dashboard on a specific FortiGate model.
1151300	Logs are not displayed in FortiGate CLI when using free-style filter with timestamp and FortiAnalyzer as data source.

Proxy

Bug ID	Description
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.
1118701	Connection issues for Kentik application using http2 gRPC occur with proxy and deep inspection.
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.

Bug ID	Description
1141948	Certificate inspection profiles differ across VDOMs when importing policy packages from FMG, caused by inconsistent default values for unsupported-ssl-version in certificate-inspection profiles between different FOS releases.
1144571	TLS handshake fails when Client Hello is split across two packets in proxy-mode, and the packet length is less than 256 bytes.
1146601	With proxy inline-ips, a memory leak occurs on the WAD daemon, leading to conserve mode.
1155170	Memory usage increases unexpectedly during high load when processing WAD-related tasks.
1159963	Expired server certificates are issued when Deep Inspection is enabled due to improper handling of certificate cache renewals.

Routing

Bug ID	Description
1097939	Console prints out "/bin/cmdbsvr...node=system.health-check-fortiguard.name" error messages when restoring a config.
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.
1147497	Slow performance and network issues when surfing to Internet from GRE tunnels.
1150878	The IPoE tunnel interface cannot be selected in the Interface Bandwidth widget.
1152976	Spokes using remote-as-filter with 4-byte ASN cannot establish BGP neighborship.
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.
1171689	Incorrect route selection occurs during BGP redistribution with route maps due to improper handling of parent protocol distances.

SD-WAN

Bug ID	Description
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

Bug ID	Description
1147727	Encapsulated traffic of GRE tunnel interface over VNE tunnel egressed wrong interface after reboot
1153992	Event log used wrong reason that packetloss over the threshold when SLA fails due to consecutive probes failed
1159877	Hash-mode remains visible when SD-WAN service mode is changed to priority.

Security Fabric

Bug ID	Description
1085248	FortiGate encounters CPU and memory usage issue when loading 20 large external threat feeds (100K entries each).
1117104	Scheduled automation incorrectly triggers reschedule after reboot when using specific time zones and NTP configurations.
1145138	Automation stitch fails to shut down a specific port on the secondary FortiGate during HA failover due to incorrect script environment settings.
1149817	Security Fabric > Physical Topology: FortiLink Tier 2 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.

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.
1114032	The GUI becomes slow or unresponsive when transceiver-related API requests fail.
1135460	Health status becomes unknown after renaming a switch in the switch controller on some FortiGate models.

Bug ID	Description
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	FSW/FAP/FEX registration to FortiCloud is failing via FortiGate GUI.
1138263	FortiSwitch port configurations fail to update and GUI display issues occur when user-info process overloads system resources with excessive connections.
1138430	On Switch controller, increase managed-switch.switch-id to more than 16 characters.

System

Bug ID	Description
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 (for example, IPv6) is unreachable.
908309	LLDP packets not received on management interface when LLDP is enabled on certain FortiGate models.
973034	LACPDU packet drops occur when FortiGate fails to reliably send required packets due to incorrect npu_tc assignment for hi-priority traffic.
992323, 1056133, 1075607, 1082413, 1084898, 0992323	Traffic interrupted when traffic shaping is enabled on 9xG and 12xG.
996863	Automatic firmware updates email alert after every reboot of FortiGate.
1029459	sflowd error condition occurs when sflow sampling is enabled without a collector configured.
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.
1071229	Ping reply packets are dropped after two successful requests when using VXLAN over IPsec on FortiGate.
1082891	FortiGate reboots immediately after changing ull-port-mode to 25G without a confirmation prompt.
1095801	Error "Fail to del default npu-vlink setup" is shown when changing the hostname.

Bug ID	Description
1096384	Warn user when restoring config from a different firmware version.
1099770	NP7 drops encrypted GRE packets that have Checksum bit set (1) due to invalid checksum.
1107270	Communication over VXLAN is lost after upgrade on NP7 platform.
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.
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.
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.
1121548	Enabling "device-identification" also gets endpoint information even though intermediate router exists on FG and endpoints.
1122741	Two duplicate FGFM sessions could be triggered when connecting to FortiGate Cloud. The first FGFM session that enters in GET_IP state kills the other FGFM session, which schedules an FGFM session restart two minutes later.
1130803	Port13-20 speed setting changes to 1000full after FortiGate 10xF reboot.
1132414	When connecting port5-14 on 3201F with third-party switches using optical transceivers, the 1gig link is down.
1133575	The 100M speed option is not available for wan1 and wan2 interfaces during configuration in certain FortiGate models.
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.
1140755	When attempting to delete a software switch interface, it becomes permanently hidden due to an unreverted temporary flag.
1141907	Unexpected behavior occurs when deleting IPv6 reflect session.
1142591	Unexpected behavior occurs when high load IP fragment traffic is sent through an IPsec tunnel with vpn-id-ipip encapsulation and offloading enabled.
1142782	GRE tunnel traffic is limited when sessions share same local/remote IPs, causing them to be assigned to single CPU core.
1142805	Cannot set source IP for FortiGuard when a non-root VDOM is set.
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.

Bug ID	Description
1148843	Unstable LTE 4G connection occurs when using IPv6.
1151313	On NP7 models, gtp tunnel list counters don't increase when restoring configuration file with "gtp-enhanced-mode enable".
1152059	Device information is not detected when device-detection is enabled.
1152638	FGT still sends reset packet when drops TCP SYN packets with `ident-accept enable` on wwan interface after reboot.
1153004	APN profile not updating when configuring Verizon APN.
1154158	DHCP issue occurs when configuring hardware switch interface in A-P HA mode.
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.
1160215	An error condition occurs in snmpd on FortiGate-VM64-AZURE approximately every 1.5 hours.
1163814	Memory usage issues occur when newcli processes are not deleted after their parent sshd process died.
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, such as FortiGate 480xF.

User & Authentication

Bug ID	Description
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.
1124183	Guest user sessions persist in the FortiGate authentication list despite manual expiry, enabling continued network access.
1137727	Delays in SSH login verification occur on some FortiGate models when hashing passwords, and immediate failure messages are returned for invalid usernames.
1156903	CLI authentication test fails when RADIUS server has require-message-authenticator setting disabled.

VM

Bug ID	Description
1125437	The "set distance" option under interface configured as DHCP client doesn't work on VM.
1146370	AWS bootstrap is unable to parse IAM role profile properly due to the length.
1146634	IfLinkUpDown SNMP trap is not triggered on FGT_VM64_KVM using the virtio driver when an interface is brought up or down.
1157674	Incorrect system time occurs when FortiGate-VM64-GCP boots up on GCP.

WAN Optimization

Bug ID	Description
1160444	Global config wanopt content-delivery-network-rule is deleted when restoring VDOM config.

Web Filter

Bug ID	Description
1145481	URL filter exemption fails when adding regex entries to URL filter if newly added regex entry contains invalid perl style regex.
1150232	Threat feed URLs are not blocked since Sandbox block list file version check always fails and aborts loading other types of URL lists, 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.

WiFi Controller

Bug ID	Description
1001211	Add optional antenna support for K-series models 443K and 243K.

Bug ID	Description
1018895	Clients on local-bridging SSIDs appear offline despite having active traffic when acd-process-count is 2, caused by the AP failing to report client IPs to the controller.
1063976	Empty SN values occur in AP DTLS session timeout messages.
1126824	When WiFi client enables VPN endpoint, VPN traffic cannot pass through NP6Xlite FGT models.
1131094	The iPhone 16 fails to connect to a WPA3-SAE SSID on FWF-61F due to incorrect ordering of RSN and RSNXE parameters during the authentication handshake.
1145326	In non-root VDOM, device fails to authenticate when MPSK is used with an external RADIUS server.
1147416	Samsung S22 cannot connect WPA3-SAE SSID from local-radio of FWF-70G.
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
1161023	Groups of Wi-Fi clients are lost after roaming to a different AP, causing unintended behavior in network policies.
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.

ZTNA

Bug ID	Description
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.
1159018	ZTNA agentless not working on FG-90G devices.

Known issues

Known issues are organized into the following categories:

- New known issues on page 52
- Existing known issues on page 53

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 7.6.4.

Agentless VPN (formerly SSL VPN web mode)

See also SSL VPN tunnel mode replaced with IPsec VPN on page 13.

Bug ID	Description
1173772	Unable to connect to SMB over SSL VPN web mode in FIPS-CC mode.

FortiGate 6000 and 7000 platforms

Bug ID	Description
1162187	Sometimes upgrade of FortiAP failed from FortiGate 7000F.
1171183	The Global Traffic widget does not load after factory reset because legacy authentication is disabled by default.
1185009	Traffic coming on a VLAN interface is dropped on FPMs due to DA_MISS_UC_DROPs in NP7.
1185869	Multicast traffic not working.
1188338	Sometimes IPv6 MLD state of interface changes to "Stopped" on primary FIM and causes all mcast6 traffic to fail.
1183709	SD-WAN health check randomly fails during automation.

GUI

Bug ID	Description
1193206	Faceplate keeps loading when editing interface.

Hyperscale

Bug ID	Description
1151441	On FG-4801F-HA, ha2 port as hw-session-sync-dev shows out-of-sync even though it is connected to NP7.

IPsec VPN

Bug ID	Description
1192598	IPsec phase1-interface option 'loopback-asymroute' is noy available for IKEv1.

VM

Bug ID	Description
1194713	ARM_KVM/GCP/OCI unable to format shared data partition on ARM VMs.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS 7.6.4.

Application Control

Bug ID	Description
1144469	No security events logged for custom Application Control profiles in Monitor mode when applied to policies configured to log all sessions.

Endpoint Control

Bug ID	Description
1019658	On FortiGate, not all registered endpoint EMS tags are displayed in the GUI.
1038004	FortiGate may not display the correct user information for some FortiClient instances.

Explicit Proxy

Bug ID	Description
1145590	certificate-inspection dropping client hello segment when traffic is tunneled in webproxy.

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.
990528	When searching for an IP address on the *Firewall Policy* page, the search/filter functionality does not return the expected results.

FortiGate 6000 and 7000 platforms

Bug ID	Description
653335	SSL VPN user status does not display on the FortiManager GUI.
835847	Password policy was not correctly updated when using automation stitch.
936320	When there is a heavy traffic load, there are no results displayed on any *FortiView* pages in the GUI.
950983	*Feature Visibility* options are visible in the GUI on a `mgmt-vdom`.
994241	On FortiGate 7000F using FGSP and FGCP, when TCP traffic takes an asymmetric path, the TCP ACK and data packets might be dropped in NP7.
1006759	After an HA failover, there is no IPsec route in the kernel. **Workaround**: Bring down and bring up the tunnel.
1102072	On the FortiGate 7000 platform, cmdbsvr CPU usage can be higher than normal for extended periods on one or more FPM.

Bug ID	Description
1112582	Under some conditions, such as during conserve mode, you may be unable to log in to the FortiGate 6000 management board GUI or CLI, or when you log in to the management board console, a message similar to fork failed() continuously repeats.
1130491	6KF WCCP doesn't seem to work as expected.
1131269	Dial up tunnel - syn and syn ack are on different blades even though ipsec-tunnel-slot set to master.
1132294	ip nat port-preserve feature is not working when client's source port doesn't fall under FPM's nat port-range.
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
1034148	The *Application Bandwidth* widget on the *Dashboard > Status* page does not display some external applications bandwidth data.

GUI

Bug ID	Description
793029	Unexpected behavior occurs on some FortiGate models when a FortiClient lacks a required MAC address attribute.
1047146	After a firmware upgrade, a VLAN interface used in IPsec, SSL VPN, or SD-WAN is not displayed on the interface list or the SD-WAN page and cannot be configured in the GUI.
1112727	Force FortiCare/FortiCloud registration, only allow exception from a new BIOS setting.
1140785	GUI packet capture displays incorrect information.

HA

Bug ID	Description
851743	When running the `diag sys ha checksum cluster` command, a previous line result is added further down in the output instead of new line result when a FortiGate is configured with several VDOMs .

Hyperscale

Bug ID	Description
1030907	With a FGSP and FGCP setup, sessions do not show on the HA secondary when the FGSP peer is in HA.
1042011	Observed `NPD-0 :DEL PRP FAIL! 0xffffffff; NPD-0 :PRP ADD FAIL! 0xffffffff nat_type=00000044 block_sz=128 port_base=11000`.
1130107	Session-helper DNS session is created by hw and can be seen in log2host table.

Intrusion Prevention

Bug ID	Description
1076213	FortiGate's with 4GB memory might enter conserve mode during the FortiGuard update when IPS or APP control is enabled. **Workaround**: Disable the `proxy-inline-ips` option under `config ips settings`.
1093769	Unexpected IPS UTM log has been generated for established TCP sessions that lack application data in NFGW policy mode.
1140846	Unexpected behavior observed in the IPSEngine when handling HTTPS traffic using HTTP/2 in certain configurations.

IPsec VPN

Bug ID	Description
735398	On FortiGate, the IKE anti-replay does not log duplicate ESP packets when SA is offloaded in the event log.
944600	CPU usage issues occurred when IPsec VPN traffic was received on the VLAN interface of an NP7 vlink.
1042371	RADIUS authentication with EAP-TLS does not work as expected through IPsec tunnels.

Log & 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.
1124896	FAZ and FGT-cloud *Logs Sent Daily* chart looses data after upgrade.

Proxy

Bug ID	Description
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
938349	Unsuccessful API user login attempts do not get reset within the time specified in `admin-lockout-threshold`.
993345	The router API does not include all ECMP routes for SD-WAN included in the `get router info routing-table` command.
1103046	Shaping profile with queuing - no interface stats.

Security Fabric

Bug ID	Description
1040058	The Security Rating topology and results does not display non-FortiGate devices.

Switch Controller

Bug ID	Description
1113304	FortiSwitch units are offline after FortiGate is upgraded from 7.4.6 or 7.6.0 to 7.6.1 or later when LLDP configuration is set to vdom/disable under the FortiLink interface. **Workaround**: In LLDP configuration, enable `lldp-reception` and `lldp-transmission` under the FortiLink interface, or rebuild the FortiLink interface.

System

Bug ID	Description
947982	On NP7 platforms, DSW packets are missing resulting in VOIP experiencing performance issues during peak times.
1012577	Traffic on WAN interface is dropped when policy-offload-level (under config system setting) is set to dos-offload.
1041726	Traffic flow speed is reduced or interrupted when the traffic shaper is enabled.
1047085	The FortiOS GUI is unresponsive due to a CPU usage issue with the `csfd` and `node` processes.
1058256	On FortiGate, interfaces with DAC cables remain down after upgrading to version 7.4.4.
1075911	Traffic randomly stops working through an Aggregate interface.
1103617	Integrating an interface does not work when adding a new member into an existing interface or creating a new interface.
1142465	ARP entries age out quickly after a system reboot, despite a long reachable-time setting.
1145397	security-exempt-list not retaining its structured rule set when editing an interface configuration through the GUI.

Upgrade

Bug ID	Description
1091213	Upgrade causes X5 & X7 SFP Interfaces to go down.

User & Authentication

Bug ID	Description
1021719	On the *System* > *Certificates* page, the *Create Certificate* pane does not function as expected after creating a new certificate.
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.
1141380	FortiGate cannot send token activation code to email.

VM

Bug ID	Description
1125805	Unable to access the FortiGate VM web interface deployed on AWS when ACME is enabled.

Web Filter

Bug ID	Description
1040147	Options set in `ftgd-wf` cannot be undone for a web filter configuration.
1058007	Web filter custom replacement messages in group configurations cannot be edited in FortiGate.
1074960	Internet connectivity slowness in policy in proxy mode inspection and webfilter profile (increase of NP7 drop counters observed).

Built-in AV Engine

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

Resolved engine issues

Bug ID	Description
937550, 1003433	In a rare situation, the file filter may mistakenly classify PDF files as BAT files, leading to an undesired blockage of these files.
1152932	Unexpected behavior observed in the AV engine, caused by erroneous memory allocation after failing to retrieve cryptographic information

Built-in IPS Engine

IPS Engine 7.01154 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

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