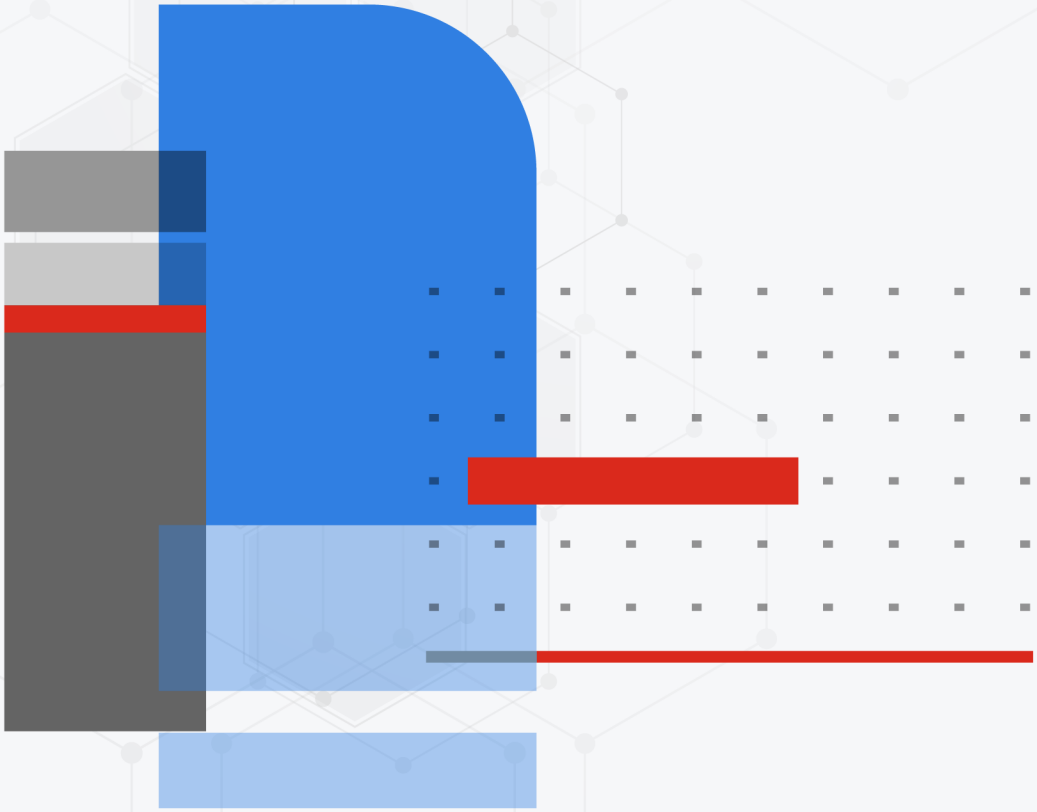
Release Notes

FortiProxy 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

October 15, 2025
FortiProxy 7.4.9 Release Notes
45-749-1153329-20251015

TABLE OF CONTENTS

Change log

Date	Change Description
2025-05-07	Initial release.
2025-06-10	Added CVE-2025-22862 to Resolved issues on page 15.
2025-07-09	Added CVE-2024-55599 and CVE-2024-52965 to Resolved issues on page 15.
2025-10-15	Added CVE-2025-22862, CVE-2025-25253, and CVE-2025-54822 to Resolved issues on page 15.

Introduction

FortiProxy delivers a class-leading Secure Web Gateway, security features, unmatched performance, and the best user experience for web sites and cloud-based applications.

FortiProxy 7.4.9 supports upgrade from 7.4.x only. Refer to Deployment information on page 11 for detailed upgrade instructions.

All FortiProxy models include the following features out of the box:

Security modules

The unique FortiProxy architecture offers granular control over security, understanding user needs and enforcing Internet policy compliance with the following security modules:

Web filtering	The web-filtering solution is designed to restrict or control the content a reader is authorized to access, delivered over the Internet using the web browser. The web rating override allows users to change the rating for a web site and control access to the site without affecting the rest of the sites in the original category.
DNS filtering	Similar to the FortiGuard web filtering. DNS filtering allows, blocks, or monitors access to web content according to FortiGuard categories.
Email filtering	The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages. Updates to the IP reputation and spam signature databases are provided continuously by the FDN.
CIFS filtering	CIFS UTM scanning, which includes antivirus file scanning and DLP file filtering.
Application control	Application control technologies detect and take action against network traffic based on the application that generated the traffic.
Inline CASB	The inline CASB security profile enables the FortiProxy to perform granular control over SaaS applications directly on policies.
Data Loss Prevention (DLP)	The FortiProxy DLP system allows you to prevent sensitive data from leaving your network.

Antivirus	Antivirus uses a suite of integrated security technologies to protect against a variety of threats, including both known and unknown malicious codes (malware), plus Advanced Targeted Attacks (ATAs), also known as Advanced Persistent Threats (APTs).
SSL/SSH inspection (MITM)	SSL/SSH inspection helps to unlock encrypted sessions, see into encrypted packets, find threats, and block them.
Intrusion Prevention System (IPS)	IPS technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.
Zero Trust Network Access (ZTNA)	ZTNA is an access control method that uses client device identification, authentication, and Zero Trust tags to provide role-based application access. It gives administrators the flexibility to manage network access for users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using Zero Trust tags.
Content Analysis	Content Analysis allow you to detect adult content images in real time. This service is a real-time analysis of the content passing through the FortiProxy unit.
Client-based native browser isolation (NBI)	Client-based native browser isolation (NBI) uses a Windows Subsystem for Linux (WSL) distribution (distro) to isolate the browser from the rest of the computer in a container, which helps decrease the attack surface.

Caching and WAN optimization

All traffic between a client network and one or more web servers is intercepted by a web cache policy. This policy causes the FortiProxy unit to cache pages from the web servers on the FortiProxy unit and makes the cached pages available to users on the client network. Web caching can be configured for standard and reverse web caching.

FortiProxy supports WAN optimization to improve traffic performance and efficiency as it crosses the WAN. FortiProxy WAN optimization consists of a number of techniques that you can apply to improve the efficiency of communication across your WAN. These techniques include protocol optimization, byte caching, SSL offloading, and secure tunneling.

Protocol optimization can improve the efficiency of traffic that uses the CIFS, FTP, HTTP, or MAPI protocol, as well as general TCP traffic. Byte caching caches files and other data on FortiProxy units to reduce the amount of data transmitted across the WAN.

FortiProxy is intelligent enough to understand the differing caching formats of the major video services in order to maximize cache rates for one of the biggest contributors to bandwidth usage. FortiProxy will:

- Detect the same video ID when content comes from different CDN hosts.
- Support seek forward/backward in video.
- Detect and cache separately; advertisements automatically played before the actual videos.

What's new

The following sections describe new features, enhancements, and changes in FortiProxy 7.4.9:

Traffic shaping based on HTTP response

FortiProxy 7.4.9 introduces the new response shaping policy, which is a specialized type of traffic shaping policy that works on the top of a traffic shaping policy to further match the traffic based on certain HTTP response header fields. When *Http Response Match* is enabled in a traffic shaping policy, any traffic that matches the traffic shaping policy is further evaluated against the list of response shaping policies. If a match is found, the traffic will be mapped to the traffic shaper or assigned to the class defined in the response shaping policy instead of the ones defined in the original matching traffic shaping policy.

See Traffic shaping based on HTTP response in the Administration Guide for an end-to-end configuration example.

IKEv2 support for IPsec VPN

FortiProxy7.4.9 adds IKEv2 support for IPsec VPN.

Increase proxy-address configuration limit

FortiProxy 7.4.9 includes the following changes to the proxy-address configuration limit for VM04 and VM08:

Proxy address object	New configuration limit for 7.4.9
Proxy Address Object	80K
Proxy Address Group	4096
Proxy Address Group Member	30K

CLI changes

FortiProxy 7.4.9 includes the following CLI changes:

- `config system global`—Use the new `set tcp-random-source-port` subcommand to enable or disable (default) TCP IPv4 random source port.
- `config webfilter urlfilter`—Use the new `set include-subdomains` subcommand to enable (default) or disable (default) matching subdomains.
- `config firewall policy`—Use the new `set https-sub-category` option to enable or disable HTTPS sub-category policy matching. The default is disable.
- `config web-proxy global`—The `set policy-category-deep-inspect` option is removed.
- `config system global`—Use the new `set kernel-panic-on-warn` subcommand to configure whether to enable kernel panic and reboot when a kernel warning is issued.
- `config system replacemsg http`—The `msg-type` parameter includes the new `videofilter-block-text` option that you can use to customize the replacement message for video filter.

  Example:

  ```
  config system replacemsg http "videofilter-block-text"
     set buffer "Video access blocked by FortiProxy."
     set header 8bit
     set format text
  end
  ```
- `config firewall access-proxy`—Use the new `set verify-cert` subcommand to configure whether to enable certificate verification.
- `config system password-policy`—Use the new `set login-lockout-upon-downgrade` subcommand to configure whether to lock out login of administrative users upon downgrade.
- `config router static`—Use the new `set preferred-source` subcommand to configure the preferred source IP for the route.
- `diagnose sys filesystem tree`—Use this new command to list the top files/folders tree.
- `diagnose sys filesystem hash`—Use this new command to generate hash for files within the filesystem. See Computing file hashes in the Administration Guide for more details.
- `diagnose system filesystem last-modified-files`—Use this new command to list the last modified files.
- `diagnose sys session list-verbose`—Use this new command to list sessions in verbose detail.
- `diagnose sys mpstat`—Use this new command to diagnose mpstat.

Product integration and support

The following table lists product integration and support information for FortiProxy 7.4.9 build 670:

Type	Product and version
FortiProxy appliance	• FPX-400E • FPX-2000E • FPX-4000E • FPX-400G • FPX-2000G • FPX-4000G
FortiProxy VM	• FPX-AZURE • FPX-HY • FPX-KVM • FPX-KVM-ALI • FPX-KVM-AWS • FPX-KVM-GCP • FPX-KVM-OPC • FPX-VMWARE • FPX-XEN
Fortinet products	• FortiOS 6.x and 7.0 to support the WCCP content server • FortiOS 6.0 and 7.0 to support the web cache collaboration storage cluster • FortiManager - See the FortiManager Release Notes. • FortiAnalyzer - See the FortiAnalyzer Release Notes. • FortiSandbox and FortiCloud FortiSandbox- See the FortiSandbox Release Notes and FortiSandbox Cloud Release Notes. • FortiIsolator 2.2 and later - See the FortiIsolator Release Notes.
Fortinet Single Sign-On (FSSO)	5.0 build 0301 and later (needed for FSSO agent support OU in group filters) • 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

Type	Product and version
	• Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
Web browsers	• Microsoft Edge • Mozilla Firefox version 87 • Google Chrome version 89  Other web browsers may work correctly, but Fortinet does not support them.
Virtualization environments	Fortinet recommends running the FortiProxy VM with at least 4 GB of memory because the AI-based Image Analyzer uses more memory compared to the previous version.
	Hyper-V: • Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022
	Linux KVM: • RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
	Xen hypervisor: • OpenXen 4.13 hypervisor and later • Citrix Hypervisor 7 and later
	VMware: • ESXi versions 6.5, 6.7, 7.0, and 8.0
	Openstack: • Ussuri
	Nutanix: • AHV
Cloud platforms	• AWS (Amazon Web Services) • Microsoft Azure • GCP (Google Cloud Platform) • OCI (Oracle Cloud Infrastructure) • Alibaba Cloud

Deployment information

You can deploy the FortiProxy on a FortiProxy unit or VM. You can also upgrade or downgrade an existing FortiProxy deployment. Refer to Product integration and support on page 9 for a list of supported FortiProxy units and VM platforms.

Downloading the firmware file

1. Go to https://support.fortinet.com.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support* > *Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiProxy*.
5. On the *Download* tab, navigate to the FortiProxy firmware file for your FortiProxy model or VM platform in the *Image Folders/Files* section. `.out` files are for upgrade or downgrade. `.zip` and `.gz` files are for new deployments.
6. Click *HTTPS* to download the firmware that meets your needs.

Deploying a new FortiProxy appliance

Refer to the FortiProxy QuickStart Guide for detailed instructions of deploying a FortiProxy appliance. Refer to Product integration and support on page 9 for a list of supported FortiProxy units.

Deploying a new FortiProxy VM

Refer to the FortiProxy Public Cloud or FortiProxy Private Cloud deployment guides for more information about how to deploy the FortiProxy VM on different public and private cloud platforms. Refer to Product integration and support on page 9 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.4.9 supports upgrade from 7.4.x only.

If Security Fabric is enabled, all FortiProxy units must be upgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.4.9, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.9. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.

To upgrade FortiProxy units or VMs from 7.4.x to 7.4.9:

If you are using a RADIUS server that does not support the message-authenticator attribute, upgrading to 7.4.9 is not recommended.

1. Reboot the FortiProxy.

   You must reboot the FortiProxy before the upgrade process. Otherwise, the device may be damaged due to upgrade failure during critical processing.

2. In the GUI, go to *System* > *Fabric Management*.
3. Select the device you want to upgrade in the table and click *Upgrade*.
4. Click *Browse* in the *File Upload* tab.
5. Select the file on your PC and click *Open*.
6. Click *Confirm and Backup Config*.
7. Click *Continue*.

   The configuration file is automatically saved and the system will reboot.
8. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

If you are currently using FortiProxy 2.0.x, 7.0.x, or 7.2.x, Fortinet recommends that you perform the upgrade procedure for each major version in between from low to high before attempting to upgrade to 7.4.9. For example, to upgrade from 2.0.12 to 7.4.9, upgrade to 7.0.11 or later first, and then 7.2.5 or later (reboot before upgrading to 7.2.x), and then 7.4.0, and then 7.4.9.

Upgrading a FortiProxy 2.0.5 VM to 7.0.x requires a different upgrade process with additional backup and configuration as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.

To upgrade a FortiProxy 2.0.5 VM to 7.0.x:

1. Back up the configuration from the GUI or CLI. Make sure the VM license file is stored on the PC or FTP or TFTP server.
2. Shut down the original VM.
3. Deploy the new VM. Make sure that there is at least 4 GB of memory to allocate to the VM.
4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI.
6. Restore the configuration using the CLI or GUI.
7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Downgrading the FortiProxy

Downgrading FortiProxy 7.4.9 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

If Security Fabric is enabled, all FortiProxy units must be downgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.4.9, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.9. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.

You can downgrade FortiProxy units or VMs from 7.4.9 to 7.2.x by following the steps below:

1. In the GUI, go to *System > Fabric Management*.
2. Select the device you want to upgrade in the table and click *Upgrade*.
3. Click *Browse* in the *File Upload* tab.
4. Select the file on your PC and click *Open*.
5. Click *Confirm and Backup Config*.
6. Click *Continue*.

The configuration file is automatically saved and the system will reboot.

7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

To downgrade from FortiProxy 7.4.9 to 7.0.x or 2.0.x, Fortinet recommends that you perform the downgrade procedure for each major version in between from high to low before attempting to downgrade to the target version. For example, to downgrade from 7.4.9 to 2.0.12, downgrade to 7.2.5 or later first, and then 7.0.11 or later, and then 2.0.12.

Downgrading a FortiProxy 7.0.x VM to 2.0.5 or earlier requires a different downgrade process with additional backup and configuration as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.

To downgrade a FortiProxy 7.0.x VM to FortiProxy 2.0.5 or earlier:

1. Back up the configuration from the GUI or CLI. Make sure the VM license file is stored on the PC or FTP or TFTP server.
2. Shut down the original VM.
3. Deploy the new VM. Make sure that there is at least 2 GB of memory to allocate to the VM.
4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI
6. Restore the configuration using the CLI or GUI.
7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Resolved issues

The following issues have been fixed in FortiProxy 7.4.9. For inquiries about a particular bug, please contact Customer Service & Support.

Description	Bug ID
1112600	The wad_ftp_session_task_start does not initiate while establishing the data connection.
1115137	Increase the maximum value of proxy-auth-timeout from 600 to 4320 minutes.
1113152	BUFFER_SIZE found in daemon-wad - wad_chunk.c:wad_chunk_buf_get.
1114438	Policy test feature does not work when no WAD debug is running in the background.
1105419	SSL inspection is being applied even though traffic matches a policy that has no inspection.
1107077, 1107230	No buffer size checking before memory copy and move operations.
1111141	WAD process crashes continuously after ftgd-local-rating configuration.
1074460	Buffer overflow issues related to corrupted traffic log files, which could lead to a crash.
1118107	Non-HTTP traffic does not bypass app policy with deny and is dropped.
1107113	SSL exempt logs "destination" and "destination-interface" fields are incorrect.
1115595	Traffic log says utmaction="allowed" when the security profile is not configured so.
1115799	VIP does not follow policy.
1117526	list_entry should be typesafe.
1089162	In transparent mode, IP address changes on management interface is not learned until reboot.
1117013	wad_hash_cache timeout issue.
1117213	Missing return value check in upd_ips_report.c.
1115027	ICAP does not support sending SNI when FQDN is configured.
1110873, 1121008, 1122890, 1125661, 1116906, 1126935, 1133247, 1134920, 1005491, 1148955, 1098827, 1116523	GUI issues.
1119561	Update library logging defaults.

Description	Bug ID
1111239	The lock IP address function does not work in explicit proxy mode.
1054835, 1121171	Proxy HTTP2 single file transfer is slow when IPS/APP/SSL inspect-all is enabled.
924740	Improve WAD trace log precision of process-id-by-src filter.
1115120	Incorrect service and URL in AV log when HTTP request via external proxy hit the AV infected URL cache.
1121444	Create custom SaaS applications for inline CASB causes HA to be out of sync.
1125850	Fix the calculation of new buffer length.
1080366	The FURL license seat does not control the inline CASB feature.
1119389	Explicit proxy does not work via IPsec tunnel.
1103476	License leak.
1119179	WAD crash with AV profile while accessing some websites.
1128580	FortiSandbox connection status shows error "Unreachable or not authorized" after upgrade.
1095093, 1092529	"utmref" and "utmaction" fields are missing in forward traffic log and long-tcp sessions are missing in http-transaction traffic log.
1102694	"utmref" and "utmaction" fields are missing in forward traffic log and http-transaction traffic log for long-tcp sessions.
1127033	For a policy with IP pool enabled, IP pool change does not take effect unless you disable and enable IP pool in policy.
1056498, 1075806, 1109306, 1110202	Proxy inline IPS performance on HTTP traffic is much worse than the IPS engine.
1109469	FortiProxy SOCKS5 traffic is denied when detect-https-in-http-request is enabled.
1128154	"print tablesize" returns the wrong values.
1128283	Logs that should have duration 0 sometimes show wrong values.
1131180	Error message on console when FPX-4000E is booting.
1110904	Unable to see logs for traffic that matches transparent policy with action DENY.
1128653	DNS resolution and latency issues after importing FQDN address objects.
1127524	web-proxy forward-server monitor URL does not work with HTTP scheme.
1106807, 1129308	With a configuration that blocks bats.video.yahoo.com, visiting tw.sports.yahoo.com triggers HTTP2 PROTOCOL_ERROR.
1123962	`diag wad policy` list does not show implicit deny/allow policy.
985311, 1121357,	X-Forwarded-For header in webfilter log and "exec tac report" trace on console.

Description	Bug ID
1110850	
1048296	Error in the HTTP2 framing layer when accessing a specific website via proxy with deep inspection configured.
1126862	Traffic is passed by transparent deny policy when log-http-transaction is enabled.
1130067	HTTP/2 traffic cannot pass through the explicit-policy when web filter is enabled.
1133565	Password protected msofficex and msoffice files are bypassed when encrypted-file is set to inspect.
1127352	Inline-IPS duplicate and conflicting app control logs.
1126749	Duplicate session ID in traffic logs across different connections.
1137505	If the LDAP returns a user with group "a", it will match group "a1", "a2", which is incorrect.
1096529	WAD crash at wad_ctrl_workers_close_ips_db once.
1135709	Ipset is unable to handle maximum external resource size.
1125699	Inline IPS PCRE pattern matching issues.
1102796	Passive proxy member send LDAP requests to the LDAP servers.
1104821	WAD has signal 6 crash at wad_ftp_data_session_make.
1012742	With fast-policy-match enabled, proxy fails to match policy for traffic with SD-WAN logical interface index.
1121249	CASB fails to block the HTTP request when CASB profile is enabled and the header name is a known header like "Accept", "Content-type", "User-Agent", or "Host" set header-name "user-agent".
1134310	SSL exemption not working on policy in case of partial match.
1142196	Cannot perform DNS lookup in VDOMs in transparent mode unless a DNS server is specified.
1133901	Improve HTTP CONNECT response when "https-replacement-message" is disabled.
1138959	For parameterized signatures, inline IPS does not include parameter value in the message field of utm app log.
1111368, 1142863, 1143212	Source IPs are banned without any quarantine features enabled.
1135096	In HTTP transaction log, when certificate inspection is set, the URL filed lost protocol information if traffic passes through.
1139414	WAD signal 11 crash with "wad_mem_free".
1096529	WAD crash at wad_ctrl_workers_close_ips_db once.
1070388	FortiProxy does not respond to an ICMP request from directly connected interfaces.

Description	Bug ID
1130867	LDAP groups are not updated regularly in the WAD cache.
1142105	Inline-CASB shared memory has memory corruption when loading the signature with header match rules.
1144621	Unicast HA with transparent VDOM fails to sync.
1093881	Incorrect service name in inline IPS botnet log.
1130795	Wrong certificate for client certificate exchange in action deny explicit policy.
1144280	HA becomes out-of-sync after upgrading and requires a reboot to force it to sync again.
1105211	Inline IPS blocks customer application signature without generating replacement message or log.
1030015	BUFFER_SIZE found in UTM_Proxy.
1149344	Client certificate is not offered without authenticated user when ssl-client-certificate is set to static.
1147546	Kernel panic when clearing sessions.
1130882	Missing field details in http-transaction logs for deep-inspect https CONNECT traffic.
1102925	WAD ssl_cert leak in ZTNA.
1127366	Unable to coalesce TCP connection between the FortiProxy and web for multiple HTTPS requests from different clients.
1146216	Intermittent users traffic disconnection issues on FortiProxy VM after upgrading to 7.4.8 and applying a new user license.
1148949	Inconsistent behavior on the log disk GUI and CLI when the Security Fabric is enabled.
1149807	Policy lookup tool does not match source interface.
1149760	Inline-IPS does not match IPS sensor location.
1143212	The SSH fingerprint is changed when traffic passes through transparent mode FortiProxy.
1151886	Security Fabric devices are not shown, disconnected, and removed from configuration.
1150516, 1150517	RESOURCE_LEAK in Routing_Authentication.
1143184	Policy test does not working on service set on app-service-type app-id
1144389	Device hangs with no GUI/SSH/serial console access. Traffic processing halts completely.
1148794	Some websites were blocked by FortiProxy DLP.

Description	Bug ID
1055898	Downstream server cannot get the payload from forwarded HTTP/2 messages because Content-Length or Transfer-Encoding information is not included in the forwarded messages, which can also cause HTTP smuggling attack.
1012811	Log time is one hour behind NTP after daylight savings time change.
1140953	HTTP2 large file download may get stuck and fail.
1148219	Server IPs are missing from the admin trusted hosts.
1121980	Inline IPS blocks some LinkedIn pages that should be allowed.
1146601	Inline IPS raw scan can leak memory.
1149337	IPsec tunnel does not forward traffic for certain interface port configurations.
1152772	In non-transparent mode, enabling DNS protection for HTTP/HTTPS traffic causes the traffic to hang.

Common vulnerabilities and exposures

FortiProxy 7.4.9 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1125742	CVE-2025-22862
1117346	CVE-2024-55599
1121042	CVE-2024-52965
1125742	CVE-2025-22862
1109747	CVE-2025-25253
928124	CVE-2025-54822

Known issues

FortiProxy 7.4.9 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1108489	Safe search does not work when configured in webfilter-profile and image-analyzer-profile in local ICAP server.
1091155	DNS resolution issues logged as "Request URL DNS resolve failure".
1096536	FortiProxy stop processing traffic after VIP modification.
996875	Traffic is failing because the replacement certificate created by FortiProxy during DPI does not contain CRL or OCSP.
1005060	Ingress traffic shaper hits a bandwidth throttle that cannot be more than 2.5 Gbps. **Workaround:** Use egress shaper for better scalability.

www.fortinet.com