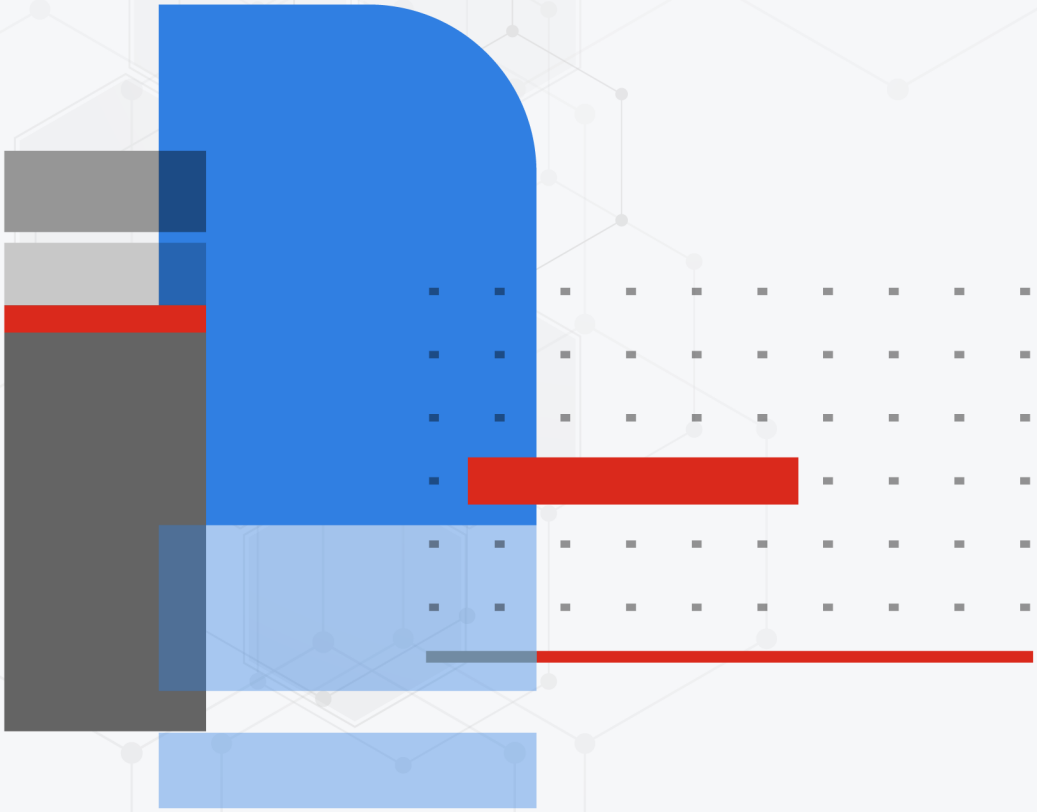
Release Notes

FortiProxy 7.4.7



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

May 21, 2025
FortiProxy 7.4.7 Release Notes
45-747-1106686-20250521

TABLE OF CONTENTS

Change log

Date	Change Description
2024-12-13	Initial release.
2025-01-15	Updated Deployment information on page 14.
2025-03-11	Added CVE-2024-45324 to Resolved issues on page 18.
2025-05-21	Updated What's new on page 7.

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 7.4.7 supports upgrade from 7.4.x only. Refer to Deployment information on page 14 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:

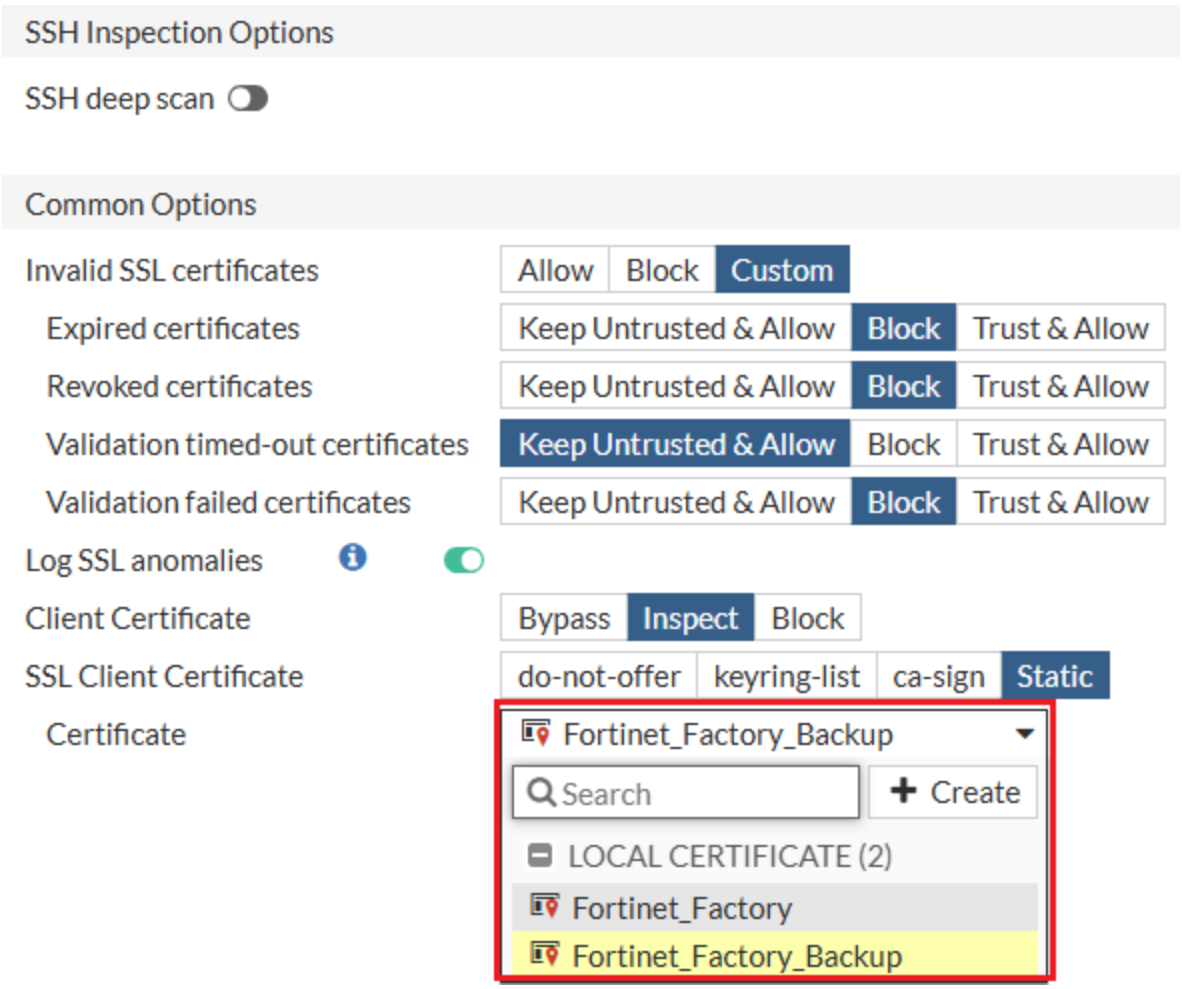
- Detect the same video ID when content comes from different CDN hosts.
- Support seek forward/backward in video.
- Detect and cache separately; advertisements automatically played before the actual videos.

What's new

The following sections describe new features, enhancements, and changes in FortiProxy 7.4.7:

Use a static client certificate for SSL/SSH inspection

When configuring an SSL/SSH inspection profile, you can now configure FortiProxy to use a static client certificate for mTLS authentication on behalf of all users using the new *Static* option of *SSL Client Certificate*. You can then select the client certificate to use.



Alternatively use the new `static` status option of the `config ssl-client-certificate` subcommand under `config firewall ssl-ssh-profile`. You can then configure the client certificate using the new `set cert` subcommand.

Header replacement in web-proxy profile

In web-proxy profiles, the header can be replaced.

```
config web-proxy profile
                        edit my_profile
                        config headers
                        edit 1
                        set name "server"
                        set action add-to-response
                        set add-option {replace | replace-when-match}
                        set content "content_changed"
                        next
                        end
```

```
                next
            end
```

`replace`	Replace content to existing HTTP header or create new header if HTTP header is not found.
`replace-when-match`	Replace content to existing HTTP header.

Support for Securosys Primus HSM

FortiProxy 7.4.7 adds support for Securosys Primus HSM.

- Under `config system nethsm`, you can now configure the HSM vendor to be Securosys Primus and then configure the Primus-related settings:

```
config system nethsm
   set status enable
   set vendor primus
   set primus-cfg <primus.cfg file content>
   set secret-content <Encrypted Config>
   config partitions
      edit "PRIMUSDEV270"
         set slot-id 1
         set pkcs11-pin <Encrypted password>
   next
end
```

- When configuring local keys and certificates using the `config vpn certificate local`command, you can now configure the HSM vendor to be Securosys Primus HSM and configure the HSM key type.
- You can perform operations on Primus HSM using the new `execute nethsm primus` command.

Add license information in SNMP

FortiProxy 7.4.7 adds license information to SNMP with the following OIDs:

- **FortiProxy license related**: 3.6.1.4.1.12356.101.10.117.*
- **SWG Bundle (FURL)**: 3.6.1.4.1.12356.101.10.117.1.*
  - **Licensed sessions**: 3.6.1.4.1.12356.101.10.117.1.1
  - **Active sessions (licensing limit)**: 3.6.1.4.1.12356.101.10.117.1.2
  - **Purchased seats**: 3.6.1.4.1.12356.101.10.117.1.3
- **Browser Isolation (FNBI)**: 3.6.1.4.1.12356.101.10.117.2.*
- **Content Analysis (FCAS)**: 3.6.1.4.1.12356.101.10.117.3.*

SR-IOV support on Hyper-V

FortiProxy 7.4.7 adds support for SR-IOV on Hyper-V to optimize FortiProxy-VM performance.

CLI changes

FortiProxy 7.4.7 includes the following CLI changes:

- `config vpn certificate local`—This command adds support for Securosys Primus HSM with the following changes:
  - Use the new `hsm-vendor` subcommand to configure the HSM vendor.

`safenet`	Safenet HSM.
primus	Securosys Primus HSM.

  - Use the new `hsm-keytype` subcommand to configure the HSM key type.

rsa	RSA key type.
ec	EC key type.

  - The `nethsm-slot` command is renamed `hsm-slot`.
- The `execute nethsm` command is renamed `execute nethsm safenet`.

  Use the new `execute nethsm primus` command to perform operations on Primus HSM with the following options:

  ```
  # execute nethsm primus
    clear-pkcs-provider-log Clear logs from /tmp/pkcs11.log, generated by pkcs11.so, the
        OpenSSL provider.
    clear-primus-log Clear logs from /tmp/primus.log, generated by libprimusP11.so.
    delete-object Delete Hardware Security Module object(s).
    dump-pkcs-provider-log Dump logs from /tmp/pkcs11.log, generated by pkcs11.so, the
        OpenSSL provider.
    dump-primus-log Dump logs from /tmp/primus.log, generated by libprimusP11.so.
    inspect-primus-library-info Display information about the integrated libprimusP11.so
        library.
    list-objects List Hardware Security Module objects.
    upload-primus-cfg Upload nethsm primus.cfg file.
    upload-primus-cfg-raw Upload nethsm primus.cfg file.
  ```

- `config system nethsm`—The `set vendor` parameter includes the new `primus` option to configure the HSM vendor to be Securosys Primus. You can then configure the Primus-related settings:

  ```
  config system nethsm

    set status enable
    set vendor primus
    set primus-cfg <primus.cfg file content>
    set secret-content <Encrypted Config>
    config partitions
  ```

```
      edit "PRIMUSDEV270"
         set slot-id 1
         set pkcs11-pin <Encrypted password>
   next
end
```

- `config firewall ssl-ssh-profile`—The `set client-certificate` subcommand adds the new `bypass-on-cert-req` option to configure FortiProxy to bypass on certificate requests.
- `diagnose debug kernel log`—Use this new command to show or clear kernel log.

`show`	Dump the kernel log.
`clear`	Clear the kernel log.

Product integration and support

The following table lists product integration and support information for FortiProxy 7.4.7 build 644:

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 • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)

Type	Product and version
	• 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 12 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 12 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 12 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.4.7 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 7.4.7, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.7. 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 7.4.7:

If you are using a RADIUS server that does not support the message-authenticator attribute, upgrading to 7.4.7 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 7.4.7. For example, to upgrade from 2.0.12 to 7.4.7, 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 7.4.7.

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 7.4.7 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 7.4.7, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.7. 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 7.4.7 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 7.4.7 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 7.4.7 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 7.4.7. For inquiries about a particular bug, please contact Customer Service & Support.

Description	Bug ID
1087908	No authentication popup when ldap-user-cache is enabled.
1084141	Cannot establish signature authmethod with IPsec.
1090073	Incorrect product name in the readme file of VMWare .ovf.zip.
1073651	"dot.quic" in no-inspection profile is not updated to bypass when the FortiProxy is first installed.
1088776	Digest auth crash.
1088339	Webfilter not blocking static URL list if 204 response is enabled.
1020828	WAD HTTP2 Stream Error when client send a small concurrent stream and make multiple concurrent requests.
1088412	No URL in the auth failed event log.
1088519	WAD does not check BOTNET when inline IPS is disabled.
1083357	Application Control does not block SharePoint upload.
1083359	Missing client IP in denied explicit forward traffic log.
1093624	Proxy regular expression and wildcard local URL filter pattern issues.
1091016	Config-sync HA cluster is out of sync after upgrade due to "authentication.setting.update-time".
1087486	ICAP client does not do URI encoding when converting FTP to HTTP.
537134	Session is not terminated after web-filter quota is reached.
1018780, 1023127	WAD crash on wad_http_avscan_comfort.
978602, 1066078, 1066567	Inline IPS and IPS engine redirection issues.
1089193	FortiProxy failed to communicate with RADIUS server that lacks message-authenticator support.
1083188, 1089697	Proxy AV does not generate infected-URL cache entry if the first request is HTTP/2.
1078395	Upgrade libnetfilter_conntrack to include the coverity fixes.
1092324	Randomly the auth portal is not displayed in the secondary.
1095945	Cannot reset one of the scanunit debugs, which permanently floods the CLI with output.

Description	Bug ID
1085179	Channel video cannot be blocked by proxy-inline-ips scan when user directly visits the video by URL.
1093671	Policy route with port configured causes IP tables failure.
1091669	CMDBError with Active-Passive config and Management Interface Reservation per WebUI
1094396	session-sync-dev is unsupported and should be hidden in CLI.
1005867, 1087631	AV scan does not work for archived msoffice, msofficex and 7z files.
1096348	Unexpected logs are generated for the known applications when the logging is disabled in application profile.
1093923	WAD crash caused by NULL webfilter profile when cmdb having issue.
1082378	The counter of bytes shows 0 after SOCKS traffic matched the policy.
1096450	WAD process crashes continuously.
1094717	Root CA certificate should be filtered out for option ssl-cert under web-proxy global.
1099891	firewall.address type wildcard does not support non-contiguous masks.
933225	Unexpected message during link monitor deamon start.
1097384	FortiProxy SOCKS policy-matching is case-sensitive while case-sensitivity is disabled globally.
1083925	When captive portal is set to FQDN, it fails to match due to FQDN case sensitivity.
1070388	FortiProxy does not respond to an ICMP request from directly connected interfaces.
1101390	Proxy-address host address config update does not take effect.
1100611	VMware kernel panic does not log to console.
1096705	With inline-IPS enabled, no SNMP traps are generated when an IPS signature is detected.
1096290	WAD crash at wad_log_http_transaction.
1103545	Serverlo ad balance VIP in policy causes IP tables failure.
1097877	The license sharing widget does not show the purchased license seats of temporarily disconnected members that are still within the 8-hour grace period.
1103035	No backward-compatibility for license sharing.
1099324	"fpx_snat_pick_ip" related kernel messages in crashlog.
1099850	WAD crashes when it tries to initialize a QUIC listener on a port that has been already assigned to another UDP listener in another daemon (e.g. DNS proxy).
1102477	Unable to download PAC file in PAC policy.
1095866	WAD not responding to clients with error when SMB uploads are blocked.
1101083	WAD app-based policy crash.

Description	Bug ID
1074493	Some HTTP Transaction logs do not contain category and category description when webfilter is enabled.
1088866	Uploading of password-protected archive files is blocked.
1100906	Source NAT shows 0.0.0.0 in the logs.
1103421	Inline IPS does not block PDF as expected.
1103965	Fails to create local certificate file.
1096728	Continuous WAD crashing on Azure which affects some VIP traffic.
983997, 1099574	Failed to validate two different CAs with the same subject and issuer.
1085418	Content analysis filename shows "Image Cache Was Cleared".
1103110, 1106077, 1094526, 1105757	GUI issues.
1105731	Add connection timeout and its handler in wad_p2s_http_sesmodule.

Common vulnerabilities and exposures

FortiProxy 7.4.7 is no longer vulnerable to the following CVE reference. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1092960, 1093060	CVE-2024-45324

Known issues

FortiProxy 7.4.7 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".
1106807	ERR_CONNECTION_CLOSED and ERR_HTTP2_PROTOCOL_ERROR occur randomly on Chrome and Edge.
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