FORTINET

Release Notes

FortiProxy 7.2.14

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

July 9, 2025
FortiProxy 7.2.14 Release Notes
45-7214--20250709

TABLE OF CONTENTS

Change log

Date	Change Description
2025-05-28	Initial release.
2025-07-09	Added CVE-2024-52965 to Resolved issues on page 14.

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. 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.
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.
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.
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.

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 7.2.14:

New FortiGuard web filter categories for AI and Cryptocurrency

FortiProxy 7.2.14 adds the following new FortiGuard web filter categories:

- **Artificial intelligence technology** (category 100): sites that offer solutions, insights, and resources related to artificial intelligence (AI).
- **Cryptocurrency** (category 101): sites that specialize in digital or virtual currencies that are secured by cryptography and operate on decentralized networks.

To configure a web filter profile to block the AI and cryptocurrency categories in the GUI:

1. Go to *Security Profiles* > *Web Filter* and click *Create New*.
2. Enter a name for the web filter profile.
3. In the category table, locate the *General Interest - Business* section. Select the *Artificial Intelligence Technology* and *Cryptocurrency* categories, and set the *Action* to *Block*.
4. Configure the remaining settings as needed.
5. Click *OK*.

CLI changes

FortiProxy 7.2.14 includes the following new commands:

- `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 7.2.14 build 0460:

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, and 7.0
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 8 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 8 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 8 for a list of supported VM platforms.

Upgrading the FortiProxy

You can upgrade FortiProxy appliances or VMs from 7.0.x or 7.2.x to 7.2.14 directly. If Security Fabric is enabled, all FortiProxy units must be upgraded to the same version. For example, if Security Fabric

is enabled in FortiProxy 7.2.14, all FortiProxy devices in the Security Fabric must run FortiProxy 7.2.14. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.

To upgrade the FortiProxy:

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 > Firmware*.
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.

If you are currently using FortiProxy 2.0.x, Fortinet recommends that you upgrade to 7.0.x first by following the same steps above before attempting to upgrade to 7.2.14.

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 7.2.14 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 7.2.14, all FortiProxy devices in the Security Fabric must run FortiProxy 7.2.14. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.

You can downgrade FortiProxy appliances or VMs from 7.2.14 to 7.2.x or 7.0.x by following the steps below:

1. In the GUI, go to *System > Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.
5. Click *Continue*.
   The configuration file is automatically saved and the system will reboot.
6. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

To downgrade from FortiProxy 7.2.14 to 2.0.x, Fortinet recommends that you downgrade to 7.0.x first by following the same steps above before attempting to downgrade to 2.0.x.

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 7.2.14. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1074460	Buffer overflow issues related to corrupted traffic log files, which could lead to a crash.
1111141	WAD process crashes continuously after ftgd-local-rating configuration.
1117526	list_entry should be typesafe.
1117013	wad_hash_cache timeout issue.
1112600	The wad_ftp_session_task_start does not initiate while establishing the data connection.
1005867, 1087631, 1088866	AV scan does not work for archived msoffice, msofficex and 7z files.
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.
1127033	IP pool is not updated after configuration change.
1119389	Explicit proxy does not work via IPsec tunnel.
1103476	License leak.
1128283	Logs that should have duration 0 sometimes show wrong values.
1094526, 1116906, 1126935	GUI issues.
1126862	Traffic is passed by transparent deny policy when log-http-transaction is enabled.
1133565	Password protected msofficex and msoffice files are bypassed when encrypted-file is set to inspect.
1126749	Duplicate session ID in traffic logs across different connections.
1102796	Passive proxy member send LDAP requests to the LDAP servers.
1140953	HTTP2 large file download may get stuck and fail.
1149807	Policy lookup tool does not match source interface.
1144421	ICAP crash.
1130882	Missing field details in http-transaction logs for deep-inspect https CONNECT

Bug ID	Description
	traffic.
1135096	In HTTP transaction log, when certificate inspection is set, the URL filed lost protocol information if traffic passes through.
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.
1157551	Memory leak caused by missing put after wad_str_assign.
859182	WAD crashed at fts_crypto_kxp_pub_key_verify_done.
1012811	Log time is one hour behind NTP after daylight savings time change.
1114438	Policy test feature does not work when no WAD debug is running in the background.
1162152	When setting system time in GUI, the *Time* field should not include the millisecond value.

Common vulnerabilities and exposures

FortiProxy 7.2.14 is no longer vulnerable to the following CVE reference. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1121042	CVE-2024-52965

Known issues

FortiProxy 7.2.14 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
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