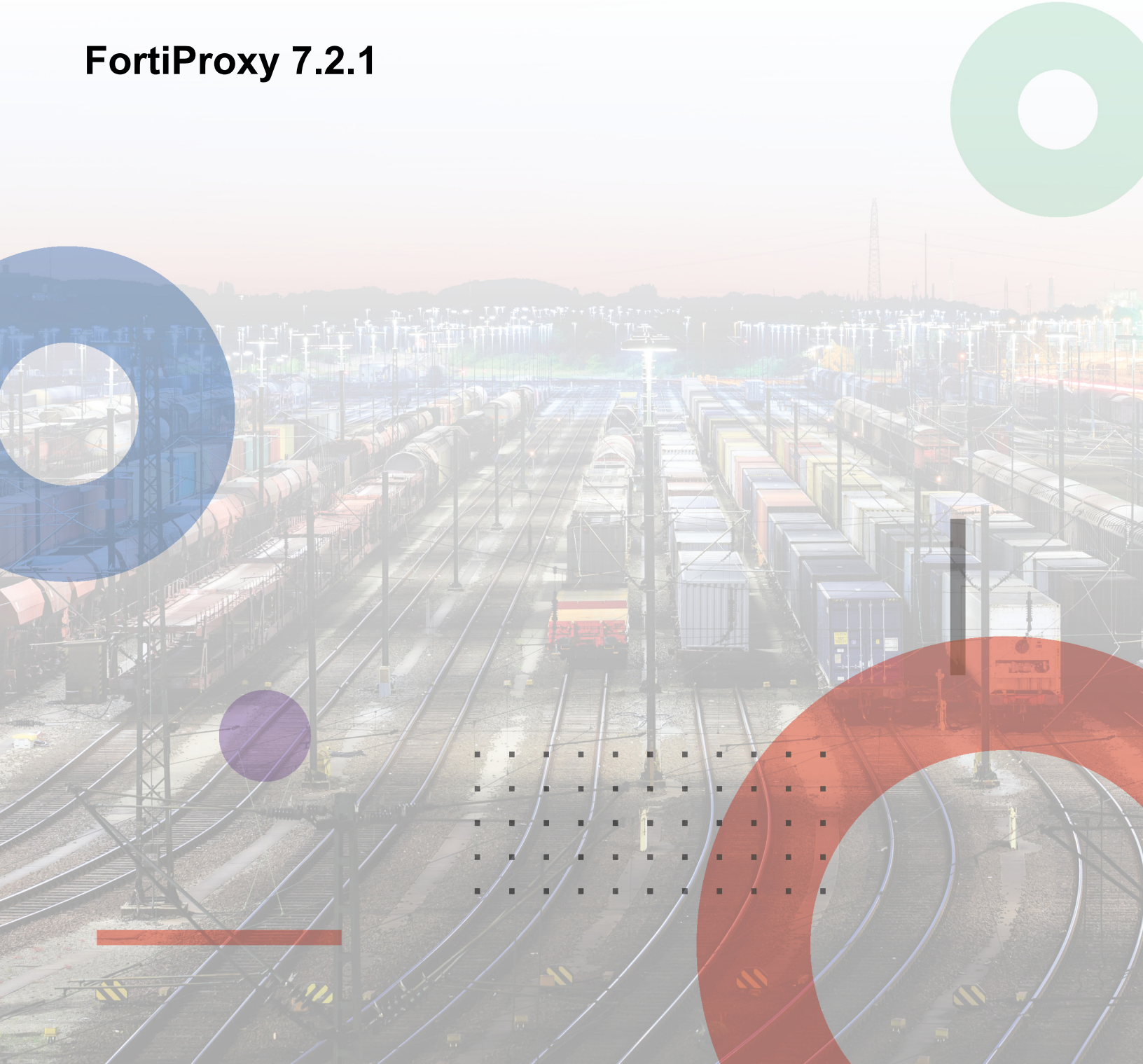
FORTINET

Release Notes

FortiProxy 7.2.1



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 26, 2023
FortiProxy 7.2.1 Release Notes
45-721-849552-20231026

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-10-07	Initial release.
2023-04-21	Updated Introduction on page 5.
2023-06-23	Updated Product integration and support on page 7.
2023-06-27	Updated Product integration and support on page 7.
2023-10-26	Updated Product integration and support 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. 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 Leak 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.

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.

Supported models

The following models are supported on FortiProxy 7.2.1, build 0300:

FortiProxy	• FPX-2000E • FPX-4000E • FPX-400E
FortiProxy VM	• FPX-AZURE • FPX-HY • FPX-KVM • FPX-KVM-AWS • FPX-KVM-GCP • FPX-KVM-OPC • FPX-VMWARE • FPX-XEN

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.2.1:

- Microsoft Edge
- Mozilla Firefox version 87
- Google Chrome version 89

Other web browsers might function correctly but are not supported by Fortinet.

Fortinet product support

- 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.

Fortinet Single Sign-On (FSSO) support

- 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)
  - Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
  - Windows Server 2008 Core (requires Microsoft SHA2 support package)
  - Novell eDirectory 8.8

Virtualization environment support

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.

HyperV	• Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019
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

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 7 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 7 for a list of supported VM platforms.

Upgrading the FortiProxy

You can upgrade FortiProxy appliances or VMs from 7.0.x or 7.2.0 to 7.2.1 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.

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 7.2.1.

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.

After you upgrade from 2.0.x to 7.0.x, click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Downgrading the FortiProxy

You can downgrade FortiProxy appliances or VMs from 7.2.1 to 7.2.0 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.

To downgrade from FortiProxy 7.2.1 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.

After you downgrade from 7.0.x to 2.0.x, click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Resolved issues

The following issues have been fixed in FortiProxy 7.2.1. For inquiries about a particular bug, please contact Customer Service & Support.

Common vulnerabilities and exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
846234	FortiProxy 7.2.1 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684
847070	FortiProxy7.2.1 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684

www.fortinet.com