FortiProxy Release Notes

Version 2.0.7

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

FORTINET®

November 19, 2021

FortiProxy 2.0.7 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
November 22, 2021	Initial release for FortiProxy 2.0.7

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 data leak prevention (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 data leak prevention 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)**
  - Intrusion Prevention System 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.

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

This release contains the following new features and enhancements.

SessionID field now available in the HTTP Transaction log

The SessionID filed has been added to the HTTP Transaction log to make it easier to correlate the HTTP Transaction log with the Forward Traffic log.

Monitoring the status of the PSUs

A log message is generated if a FortiProxy power supply unit (PSU) loses or regains power.

NOTE: This feature is available only for the FortiProxy 2000E and 4000E models.

Disabling IP-based URL rating

You can now disable the IP-based URL rating for SSL-exemption and proxy-address objects. By default, the IP-based URL rating is enabled. Use the following CLI commands:

```
config firewall ssl-ssh-profile
   edit <name>
      set ssl-exemption-ip-rating {enable | disable}
   next
end

config web-proxy global
   set address-ip-rating {enable | disable}
end
```

Supported models

The following models are supported on FortiProxy 2.0.7, build 0070:

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 2.0.7:

- Microsoft Internet Explorer version 11
- Mozilla Firefox version 61
- Google Chrome version 67

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

Fortinet product support

- FortiOS 5.x and 6.0 to support the WCCP content server
- FortiOS 5.6.3 and 6.0 to support the web cache collaboration storage cluster
- FortiAnalyzer 5.6.5
- FortiSandbox and FortiCloud FortiSandbox, 2.5.1

Software upgrade path

FortiProxy supports upgrading directly from 1.0.x, 1.1.x, or 1.2.x to 2.0.7.

Fortinet Single Sign-On (FSSO) support

- 5.0 build 0295 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

NOTE: Fortinet recommends running the FortiProxy VM with 2G+ memory because the AI-based Image Analyzer uses more memory comparing 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 6.0, 6.5, 6.7, and 7.0

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 2.0.7 or later is 2G. You must have at least 2G of memory to allocate to the FortiProxy VM from the VM host.

Upgrading the FortiProxy VM

If you are upgrading from FortiProxy 1.1.2 or earlier, including FortiProxy 1.0 to FortiProxy 2.0.7 or later, use the following procedure:

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 2G 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.

Downgrading the FortiProxy VM

Do not downgrade the FortiProxy 2.0.7 VM because the new VM license file cannot be used by earlier versions of FortiProxy.

If you are downgrading from FortiProxy 2.0.7 to FortiProxy 1.1.2 or earlier, use the following procedure:

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 2G 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.

Resolved issues

The following issues have been fixed in FortiProxy 2.0.7. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
676494	The WAN-optimization daemon (WAD) crashes when the CPU usage and the number of sessions reach their limits.
677845	Adding static URL entries in the GUI causes an internal 500 error and many static URL entries missing.
684640	When a port goes down in the HA primary unit, control was not transferred to the HA secondary unit.
726691	LACP does not work between a FortiProxy unit and a Cisco Catalyst 9500.
739382	The antivirus log shows files being oversized when they are not.
739923	The WAD causes memory usage to increase from 50% to 75% after one day.
744528	When an email with an attachment is sent from Outlook and the attachment matches the DLP sensor, the DLP sensor logs the outgoing mail direction as incoming.
744855	After upgrading from FortiProxy 2.0.5 to 2.0.6, some of the commands under `config firewall profile-group` are missing.
747417	The WAD crashes at wad_timer_list_del with signal 11 when WAN optimization is configured.
748474	Users should be able to use ISDB to block Naver Line IP addresses.
748543	After FortiProxy is rebooted, a firewall policy is missing.
748576	When basic authentication is being used in transparent mode, there are two many authentication windows being displayed.
749189	When the IP-based authentication portal is used, FortiProxy challenges the browser with 407 instead of 401.
751031	When using transparent mode, the user does not see a disclaimer when entering the user name and password.
752399	The forwarding server does not work when the destination is configured with the wildcard FQDN and proxy address.
752944	After an HA cluster is configured, LACP fails.

Bug ID	Description
753747	Users can still log in to the FortiProxy GUI, even with HTTP and HTTPS access disabled for the interface.
754275	When deep inspection and proxy authentication are enabled, the FortiProxy unit removes the server Authorization field from the HTTP header.
754298	The WAD crashes I with signal 11 when running the autotest group.
754969	The explicit FTP proxy policy selects a random destination port when the FTP client initiates the FTP session without using the default port.
755247	The WAD crashes at wad_krb_pac_send_query_resp_msg.constprop.
755365	Firefox does not show the authentication pop-up message when explicit proxy is used.
755698	When the policy is not matched, user notes should not be cleared by the HTTPS request.
755861	When upgrading FortiProxy, the units for the `proxy-auth-timeout` value need to be converted.
755892	When a user changes the HA settings, the aggregate port goes down.
756293	The aggregate interface cannot be used as the HA management interface.
757452	Traffic shaping using the Internet Service does not work.
759132	After an existing aggregate interface is deleted, the forticron application crashes.
759258	LDAPS authentication does not work from proxy users.
761352	Using the `dia deb app wad 99` command causes the WAD to crash.
761357	The WAD crashes at wad_http_session_resume_client_read_by_scan multiple times.

Common vulnerabilities and exposures

FortiProxy 2.0.7 is no longer vulnerable to the following CVEs:

- CWE-190

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

Known issues

FortiProxy 2.0.7 includes the known issues listed in this section. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
491027, 681567	Filtering the YouTube channel does not work. **Workaround:**Upgrade to FortiProxy 7.0.0.
490951	The `append explicit-outgoing-ip` command is not validated.
499787	The FortiGuard firmware versions are not listed on the *System* > *Firmware* page.