FortiProxy - Release Notes

Version 2.0.10

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

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

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

June 24, 2022
FortiProxy 2.0.10 Release Notes
45-2010-796176-20220624

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-06-24	Initial release.

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

FortiProxy 2.0.10, build 0095, is a patch release only. There are no new features and enhancements in this release. For more information, see Resolved issues on page 11.

Supported models

The following models are supported on FortiProxy 2.0.10, build 0095:

FortiProxy	• FPX-4000E • FPX-2000E • 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 2.0.10:

- 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, 1.2.x, or 2.0.x to 2.0.10.

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

Fortinet recommends running the FortiProxy VM with 4+ GB 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
Openstack	• Ussuri

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 2.0.10 or later is 4 GB. You must have at least 4 GB 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 2.0.10 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 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.

Downgrading the FortiProxy VM

⚠ Do not downgrade the FortiProxy VM 2.0.6 because the new VM license file cannot be used by earlier versions of FortiProxy.

If you are downgrading from FortiProxy 2.0.5 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 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.

Resolved issues

The following issues have been fixed in FortiProxy 2.0.10. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
784044	GCP FPX login with username=*admin* and password=<*instance-id*> keeps prompting.
787895	WAD crash when updating traffic statistic counters.
796019	Access issue with Application Control or IPS.
797270	`ha-mgmt` interface binding issue.
799718	When `to-pol` with authentication (group/user) is set to action isolate, the request fails to redirected to WAD and fails to match the given policy in the kernel.
800262	When the `auth_type` is not defined inside URL, `"GETURL("auth_type")"` is the NULL pointer. `atoi(NULL)` causes a SEGFAULT making the sslvpnd crash.
800268	When policy move-next and try-again, not set current policy, which cause use the old policy to match again.
800499	SSL/SSH Inspection and Proxy Options are missing on policy page when the action is isolate.
800873	The usage quota fills up quickly, and does not match policy bytes or FortiView user monitor traffic volume. When the usage quota limit is reached, the webfilter logs show the used quota/maximum quota value as zero.
802333	When an HTTPS connection policy match fails, it offers an implicit deny or allow policy that does not have a `sec_profile`, so `ssl_opts` is set to NULL. In certain cases this can result in a crash.
803217	Improve policy matching logic for the proxy address category.
803217	Policy matching with multiple category type proxy-address.
803452	Fast match flag is changed from enable to disable after changing settings of `profile-protocol-options`.
805210, 815851	NTLM agentless authentication fails due to user-restriction after FSSO service down.
806224	`execute ha manage` does not work for unicast HA in a FortiProxy cluster when a trusted host is configured.
807280	Proxy certificate error when no policy matched.
809832	FPX misses local-in rules for NTP server mode.
810179	Traffic shapers applied to the interface are not working as expected.
810914	Classify HTTP transaction log respond types into accurate types.
811692	NTLM authentication not working for proxy-chaining.

Bug ID	Description
813317	In transparent mode, `srcaddr-negate`, `dstaddr-negate`, and `service-negate` are available.
814398	Certificate inspection connection failures when handling TLS 1.3 with early data.
815458	IPv6 issues.
817750	WAD crash when `web-proxy.forward-server-group` does not have `server-list` configured.
820285	Masquerade setting added to `isolate-server`. It is enabled be default.