FortiProxy Release Notes

Version 2.0.9

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

April 20, 2022

FortiProxy 2.0.9 Release Notes

Revision 2

TABLE OF CONTENTS

Change log

Date	Change Description
April 15, 2022	Initial release for FortiProxy 2.0.9
April 20, 2022	Updated the “Software upgrade path” section.
May 25, 2022	Added OpenStack version support.

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 version 2.0.9, build 0086, is a patch release only. There are no new features and enhancements in this release. For more information, see Resolved issues on page 12 and Known issues on page 14.

Supported models

The following models are supported on FortiProxy 2.0.9, build 0086:

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 2.0.9:

- 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 2.0.9.

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
OpenStack	• Ussuri

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 2.0.9 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 2.0.9 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 2.0.6 VM 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 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 2.0.9. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
754289	The WAN-optimization daemon (WAD) crashes with signal 11 when running the autotest group.
768980	The `set host-regex` command is not working correctly.
770178	When a proxy address is used as the destination in a policy, unrelated traffic matches the policy.
777370	When fast-match is disabled, the HTTPS request fails to match the source proxy address in the policy.
777718	The WAD should use the port in the TCP header to match the service field.
782709	When the ICAP profile is enabled, some websites cannot be accessed.
783201	Web caching is using too much memory.
783837	After upgrading FortiProxy from an HA cluster, the primary FortiProxy license status changes to “Warning.”
784797	SSH-over-HTTP traffic is redirected to the SSH policy, even when `ssh-policy-redirect` is disabled
787496	There is a WAD memory leak.
788697	After upgrading to FortiProxy 2.0.8, when the type of destination address is set to *URL category*, the URL is blocked. **Workaround:** Use an allow policy in front of the blocking policy.
789520	When a policy has the action set to `isolate` and the service set to `http-connect`, websites are not being properly isolated.
789600	When a firewall policy has the proxy-address type set to *URL Category*, the policy does not correctly block the specified categories.
789645	The pyfcgid process crashes multiple times, causing GUI access to be lost.
789982	If the URL category is used in the firewall policy, websites are not being properly blocked.
790773	The *Old Password* is missing from the password change window.
791235	Exempting traffic from SSL inspection in the SSL/SSH inspection profile does not work.

Bug ID	Description
791242	*Malicious URLs* should not appear in the License Information.
791668	The shaping profile is not being used by the shaping policy.
792579	Implicit Deny Policy logs and HTTP transaction logs are not working.
795159	Traffic is triggering the wrong policy when the source is a proxy-address type header.
795621	When the antivirus profile is using deep inspection, some website uploads are denied.
797712	FortiProxy loses connectivity to FortiGuard, resulting in the loss of Internet access.
797915	When the `action` is set to `isolate` in an `explicit-web` firewall policy, the `profile-protocol-options` and `ssl-ssh-profile` options cannot be configured.
798054	When using deep SSL inspection, a web page produces an error but loads eventually.
798818	A WAD crash occurs with HTTP POST/PUT requests when ICAP is enabled.
799171	The WAD crashes when the configuration is being changed in a transparent firewall policy.
799214	The HTTPS request is not being forwarded to the forwarding server
799278	The `set dedicated-to management` command (under `config system interface`) is not working correctly.
800243	The management interface should only listen for ports listed in the `set allowaccess` command.
800596	When `ssh-policy-direct` is enabled, SSH-over-HTTP traffic fails to match the SSH policy.

Common vulnerabilities and exposures

FortiProxy 2.0.9 is no longer vulnerable to the following CVEs:

- CWE-120
- CWE-248
- CWE-321

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

Known issues

FortiProxy 2.0.9 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.