FortiProxy Release Notes

Version 1.0.7

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®

April 23, 2019

FortiProxy 1.0.7 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
April 23, 2019	Initial release for FortiProxy 1.0.7

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.
- **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:

- The CLI now supports x-cache-message. The `set x-cache-message` command is only available when add-x-cache is enabled. Setting the x-cache-message to an empty string makes the message the default.
- User-loaded x.509 certificates are now supported for HTTPS GUI connection and for connecting FortiProxy and FortiAnalyzer.

Supported models

The following models are supported on FortiProxy 1.0.7, build 0066:

- FortiProxy 400E
- FortiProxy 2000E
- FortiProxy 4000E
- FortiProxy VM—VMware and KVM

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 1.0.7:

- 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

Virtualization environment support

Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5

Resolved issues

The following issues have been fixed in FortiProxy 1.0.7. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
499496	SMTPS traffic containing an IPS attack should be dropped when the action is set to block it in the IPS sensor.
502631	In the HTTP transaction log, reqlength and resplength are always set to 0.
507908	WAN optimization byte-caching is not persistent.
531402	After entering memory conserve mode, the FortiProxy disks are disabled.
535204	The HD2 disk is disabled on the FortiProxy VM when using WAN optimization and logging in to the GUI.
536063	Deep inspection in explicit proxy does not work for some websites.
536857	When the inbandwidth and outbandwidth values are specified for the WAN interface, LAN clients cannot connect to the Internet.
536862	The proxy address cannot be edited in a policy.
536992	FortiManager fails to add a FortiProxy device and returns an error that the tunnel cannot be created.
537346	A disclaimer message should be displayed and acknowledged before the end user can browse the Internet.
537564	Drilling down into a policy displays an error in the GUI.

Bug ID	Description
538715	The following ciphers need to be supported in FIPS-CC mode: —TLS_RSA_WITH_AES_128_CBC_SHA —TLS_RSA_WITH_AES_256_CBC_SHA —TLS_RSA_WITH_AES_128_CBC_SHA256 —TLS_RSA_WITH_AES_256_CBC_SHA256 —TLS_DHE_RSA_WITH_AES_128_CBC_SHA —TLS_DHE_RSA_WITH_AES_256_CBC_SHA —TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 —TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 —TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA —TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA —TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 —TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 —TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA —TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA —TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 —TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
538950	The CA certificates in FortiProxy cannot be removed from the trusted store.
539251	In transparent mode, configuring multiple web proxy entries fails.
539256	In Transparent Policy mode, the Incoming IP field should not be displayed (*Policy & Objects > Explicit Policy*).
540038	If you select *Android Native* or *Windows Native* in the VPN Creation Wizard, there are “undefined” errors.
540550	On the New Address page, wildcard FQDN addresses and address groups should not be available for the host in the Proxy Address category.
540554	On the New Policy page, there should be a filter for proxy addresses and address groups for the Source field and Destination field.
541480	On the *Log > HTTP Transaction* page, the Response Time and Response Finish Time for Normal and Cached Response Type are always 0.
542230	Only one authenticated user and request should be handled by the same WAD worker.
543116	Explicit web proxy should be set to unused when not referenced.
543447	When the ICAP profile is enabled in a policy, some Internet sites are not loading.
544517	HTTP and HTTPS traffic is affected when the WAN-optimization daemon (WAD) crashes.

Bug ID	Description
544593	FTP proxy should use the interface IP address, instead of using the client IP address, to make the proxy connection between the FortiProxy unit and the FTP server.
546780	After running WAN optimization traffic, the FortiProxy VM enters memory conserve mode.
547398	After running WAN optimization traffic, the FortiProxy VM restarts by itself without any error message being displayed on the console.
547830	The `diagnose iptables shaper-stats` command displays the current bandwidth in bytes/seconds but with the units labeled as kbps.
548275	When antivirus is enabled, explicit proxy does not respond to TRACE requests.
548498	After the web filter override button is selected in the GUI, WAD crashes.
548952	When the memory is extremely low, the kernel drops any new packets.
549669	In transparent policy mode, authentication or the order of the policy rules prevents the user from reaching the destination after authentication.
549874	When ICAP is enabled and antivirus scan is disabled, the WAN-optimization daemon (WAD) crashes.
550124	After a VLAN interface was created on an aggregation, the aggregation interface cannot be deleted, even after the VLAN interface is deleted.
550407	On the *System* > *Advanced* page, the System Storage Setting does not match the setting in the CLI.
550420	The WAD crashes when visiting http://www.baidu.com.
550593	When the policy configuration changes, the WAD sometimes crashes.
550676	If the session is denied by a policy, no replacement message is displayed for some SSL web sites.
551554	The generated license file is not working on the FortiProxy 1.0 VM.
551840	When editing a policy, the proxy address is not shown in the GUI.
552284	Using a policy with the external resource IP type as the destination causes 100% CPU usage.

Common vulnerabilities and exposures

FortiProxy 1.0.7 is no longer vulnerable to the following CVEs:

- CVE-2016-6515

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

Known issues

FortiProxy 1.0.7 includes the known issues listed in this section. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

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