FortiProxy Release Notes

Version 1.0.3

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

August 15, 2018

FortiProxy 1.0.3 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
August 15, 2018	Initial release for FortiProxy 1.0.3

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 command for setting the bypass interface mode has been expanded.

  The (`set bypass`) command used to be under the `config system settings` command. To set the bypass interface mode, you can now use the following CLI commands:

  ```
  config system bypass
      set {bypass-mode | set bypass-watchdog | set bypass-timeout}
  ```

- You can now use a CLI command to find out how much memory is used by the WAN optimization daemon (WAD):

  ```
  diagnose wad memory report
  ```

- You can now use a CLI command to list the number of Kerberos authentication requests, certificate authentication requests, and NT LAN Manager (NTLM) authentication requests and responses to and from authd:

  ```
  diagnose test application wad 13
  ```

Supported models

The following models are supported on FortiProxy 1.0.3, build 0048:

- 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 1.0.3:

- 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 1.0.3. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
482785	Using a web filter profile and FortiGuard to authenticate causes the proceed and authenticate page to load slowly.
483325	After configuring two default routes, deleting one route results in deleting both routes.
490960	A zipped HLS manifest causes the FortiProxy unit to stop caching.
491821	Using HTTP POST to upload a large file through the explicit web proxy often fails.
493003,498919	The user event log does not list the user name.
493086	A user cannot change the protocol when using HTTP and a basic authentication method.
493554	When the utm-status is disabled, the profile-type and profile-group should not be available.
496294	When running explicit proxy, the FortiProxy unit is reporting 0 uptime and 0 memory usage.
498259	When running in the High Availability (HA) mode, *System* > *HA* does not show the interface status of the slave FortiProxy unit.
499487	When running explicit FTP proxy, the FortiProxy unit always lists the data traffic volume as 0 for authenticated users.
500462	When the oversize option is disabled, the FTP-over-HTTP traffic is delayed.
500965, 507155	The WAD process consumes a high amount of memory.
501020	When using a transparent proxy policy, the RSA 512-bit certificate negotiates with TLS 1.2.
503197, 504239, 505772	The WAN optimization daemon (WAD) sometimes crashes.
503478	A server response with an X-XSS-Protection header is not cached.
505249	After upgrading the firmware, firmware and drivers can no longer be downloaded when using the antivirus security profile.

Bug ID	Description
505256	When the webfilter-cache is enabled, the warning-prompt per-domain should work.
505466	The firmware upgrade from build 0043 to build 0044 fails.
505502	After upgrading, the transparent mode is slow.
506215	Traffic is intermittently block when the transparent inline mode is used.
506220	Selecting specific ports for the incoming traffic does not work with using transparent mode.
506572	Complete objects need to be deleted to improve disk storage performance.
506792	The HA Status widget on *Dashboard* > *Main* displays the HA mode as “Standalone,” instead of “Config Sync.”
506798, 506802, 506805	A Config Sync cluster synchronizes the WCCP configuration, GRE tunnel configuration, and disk settings.
506803	When configuring WCCP in the GUI, you cannot specify the ports.
507171	When using the transparent and explicit proxy, the fast-matching feature does not work.
507353	Running the active-passive HA mode causes the FortiProxy unit to become inaccessible and traffic to fail.
507365	When using the transparent mode, the outgoing interface of the transparent policy can only be set to `any` in the GUI.
507694	FortiProxy 1.0.3 is no longer vulnerable to the following CVE-Reference: CVE-2018-5390

Known issues

FortiProxy 1.0.3 includes the known issues listed in this section. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
478715	When WAN optimization crashes, the cache is not cleared.
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.