FortiProxy Release Notes

Version 1.1.2

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 10, 2019

FortiProxy 1.1.2 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
April 10, 2019	Initial release for FortiProxy 1.1.2

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:

- The *WAN Opt. & Cache* > *Prefetch URLs* page has been improved. When you select *Create New Prefetch URL*, you can schedule when URLs are preloaded, select the user agent, and specify the time between repeated preloads. You can also download the prefetch URL log.
- A new *FortiView* > *Traffic Shaping* page displays detailed information on traffic shaping.
- 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.
- You can now configure active-passive load balancing with the following commands:

```
config web-proxy forward-server-group
   edit "<forward_server_group_name>"
      set ldb-method active-passive
```

- You can now enable DNS protection for HTTP and HTTPS traffic to prevent DNS poisoning and spoofing. Use the following commands:

```
config firewall profile-protocol-options
   edit "<protocol_options_profile_name>"
      config http
         set dns-protection enable
      end
   next
end
```

Supported models

The following models are supported on FortiProxy 1.1.2, build 0162:

- 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 1.1.2:

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

Bug ID	Description
502631	The reqlength and resplength values are always 0 in the HTTP transaction log.
507908	WAN optimization byte-caching is not persistent.
526340	When using NTLM IP-based authentication, a “web proxy user limit has been reached” error is displayed.
532823	When the override is enabled on a web filter profile, the wrong FortiGuard page is displayed.
533838	Sometimes web sites are reported as having untrusted CA certificates when they have valid certificates.
534293	When visiting a blocked web site and selecting *Override*, there is no browse option in the Scope field on the GUI.
534594	When running the `diagnose sys logdisk status` and `diagnose sys logdisk smart` commands, the response is sometimes “This feature is not available on this model.”
536295	The first attempt to prefetch URLs on the reverse cache server is unsuccessful.
538886, 538887, 539256, 540550, 540554, 541120, 542682, 544258, 547800, 548165, 548936, 548937, 549916, 550407	Various features of the FortiProxy GUI need to be fixed or improved.
538906	Reordering entries in the static URL filter list using drag-and-drop does not work.
538950	The CA certificates in FortiProxy cannot be removed from the trusted store.
538953	After moving URL filter entries back and forth and then selecting *Apply*, the order of the entries submitted is not the same as the order that was arranged manually.
539251	In transparent mode, configuring multiple web proxy entries fails.
540038	If you select *Android Native* or *Windows Native* in the VPN Creation Wizard, there are “undefined” errors.

Bug ID	Description
541480	On the *Log* > *HTTP Transaction* page, the Response Time and Response Finish Time for Normal and Cached Response Type are always 0.
541539	In proxy mode, the wildcard expression in the URL filter is not matched correctly.
541984	When Kerberos authentication fails, the event log should provide more detailed information.
542230	Only one authenticated user and request should be handled by the same WAD worker.
542929	There should be a warning message when the external IP address file contains more entries than are supported.
543116	Explicit web proxy should be set to unused when not referenced.
543212	Traffic statistics should be available for HTTPS traffic handled by the transparent web proxy policy in certificate inspection mode.
544517	HTTP and HTTPS traffic is affected when the WAN-optimization daemon (WAD) crashes.
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 for about 2-3 mins, the FortiProxy VM enters memory conserve mode and stops traffic for a long time.
547398	When the WAN optimization traffic rate reaches around 60-80 transactions per second, the FortiProxy VM reboots itself without displaying an error message on the console.
548265	When the WAD worker crashes, the user information is not updated, which blocks authentication from the same IP address.
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	A user cannot reach the destination after authentication. Facebook functions cannot be controlled. Authentication is not needed for HTTP requests.
549874	When a “100 continue” response is expected, WAD crashes.
549975	After a web-filter notification is triggered by the server certificate, WAD crashes.
550124	After a VLAN interface was created on an aggregation, the aggregation interface cannot be deleted.

Bug ID	Description
550337	DNS protection does not work if HTTP policy matching is not needed.
550338	HTTP policy matching is always enabled.
550420	WAD crashed when visiting http://www.baidu.com.
550593	When the policy configuration is changed, sometimes WAD crashes.
550676	No replacement message is returned for some SSL web sites if the session is denied by a policy.

Common vulnerabilities and exposures

FortiProxy 1.1.2 is no longer vulnerable to the following CVE:

- CVE-2016-6515

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

Known issues

FortiProxy 1.1.2 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.