FortiProxy Release Notes

Version 1.0.6

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

January 28, 2019

FortiProxy 1.0.6 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
January 28, 2019	Initial release for FortiProxy 1.0.6

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 maximum number of sessions per user is now 10. For example, for a 100-user license, 1,000 proxied sessions with UTM scan are allowed. A single source IP address can use all sessions if needed.
- Two new widgets that can be displayed on the *Dashboard* > *Main* page show the numbers of logged-in users and proxied sessions over intervals from 1 minute to 24 hours.
- Link health monitoring is now supported. To use this feature, use the following CLI commands:

```
config system link-monitor
   edit "name_of_link_monitor"
      set srcintf <interface_that_receives_traffic_to_monitor>
      set server <server_IP_address>
      set protocol {ping | tcp-echo | udp-echo | http | twamp}
      set gateway-ip <xxx.xxx.xxx.xxx>
      set source-ip <xxx.xxx.xxx.xxx>
      set interval <1-3600 seconds>
      set timeout {1-255 seconds>
      set failtime <1-10>
      set recoverytime <1-10>
      set ha-priority <1-50>
      set update-cascade-interval {enable | disable}
      set update-static-route {enable | disable}
      set status  {enable | disable}
   next
end
```

- You can now allow the explicit web proxy to return packets to the interface or MAC address of the original request instead of using the route information. To control this feature, use the following CLI commands:

```
config web-proxy explicit
   edit "name_of_explicit_web_proxy"
      set return-to-sender {enable | disable}
   next
end
```

Supported models

The following models are supported on FortiProxy 1.0.6, build 0060:

- 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 1.0.6:

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

Bug ID	Description
449765, 527579, 449765, 519423, 523380, 527150, 449765, 495205, 525565, 531608, 532918	The GUI needs to be fixed.
460211	When there is a partial content response for an expired object, the WAD returns an empty reply.
502631	In the HTTP transaction log, the reqlength and resplength values are always 0.
506326	When WAN optimization is configured, the WAN optimization peer is inconsistent in blocking traffic.
507005	All members of a config-sync cluster are upgraded at the same time, instead of in sequence.
507860	The http-view report is empty.
508334	The Prefetch URL feature is not preloading entries.
509994	When using the proxy policy and deep inspection profile, the web site is denied due to a certificate error.
511161	The GUI doe not show that the first disk of the FortiProxy VM is unavailable for logging and WAN optimization. One of the disks of the FortiProxy VM is not formatted by default when FortiProxy starts.
513820	A transparent policy with authentication fails to handle HTTPS requests.
514791	Even when deep inspection is disabled, the WAN optimization client with IPS scans HTTPS requests.
515468	When SSL Nego is in active mode, the response is “500 Illegal PORT command.”
516033	The traffic log for WAN optimization data traffic shows the policy type as “policy” instead of “proxy-policy.”
516059	The source interface field in the WAN optimization traffic log should be correct.

Bug ID	Description
516254	The DLP sensor is not blocking files that are larger than the oversize limit.
516863	When more than one user is behind a NA, additional users are not prompted for authentication after the first user is successfully authenticated.
516937	When deep inspection is enabled, SSH traffic is blocked.
517909	The `mget` command does not get the files from the FTP server through the WAN optimization tunnel.
519021	If the antivirus profile is enabled on a policy, the user cannot access an application server.
521344	The explicit FTP proxy does not work with a secondary IP address.
521940	The WAD memory monitoring and debug filtering need to be improved.
522441	Some live video sites were not being cached.
523615	When the port list for a protocol is longer than 15 ports, new ports are not added.
523974	Some web sites cannot be accessed when deep inspection is enabled.
524070	The proxy address object is not working for transparent proxy traffic.
524455	The WAN optimization daemon (WAD) stops responding if the server has an untrusted certificate.
524549	SSH should be disabled by default in certificate-inspection.
524825	When a PUT or POST request is used to upload an oversized file, FortiProxy fails to respond with a 403 error.
525451	The explicit FTP proxy is not working when a request comes from a Windows FTP client or FileZilla.
525853	The routing table in an HA cluster is not synchronized when the configuration is changed when the master is down.
526363	The WAD stops responding when WAN optimization is in the active-passive mode.
526571	WAN optimization incorrectly reports that the user limit has been reached.
526840	The WAD crash log needs to be better managed.
527025	When the web portal is disabled, the FortiProxy unit redirects the HTTP client to “URL/XX/YY/ZZ/AUTH” after the HTTP client is successfully authenticated.
527579	The NTLM icon is incorrectly shown in the Method column in FortiView.

Bug ID	Description
527741	The user information is inserted into firewall authentication, even if the token is invalid.
528010	FortiProxy fails to match a policy when fast match is enabled if the URL address is an empty path.
528990	In the HTTP/HTTPS traffic log, the srcip is always 0.0.0.0, and the dstip is wrong.
529306	After client authentication, the WAD stops responding.
529553	FTP proxy failures need to be fixed.
529769	The source and destination interfac es cannot be set to “any.”
531116	FortiProxy caching collaboration is not working between two FortiProxy units in the Config-Sync (HA) mode.
531339	A wildcard FQDN object should not be able to be added in an address group in the CLI.
531377	The WAD stops responding when fast-policy-match is enabled.
531575	A web site cannot be accessed when using a web proxy policy with deep SSL inspection.
532484	When the TLS connection is terminated, FortiProxy should generate a log message.
533089	When a source peer is changed, caching collaboration fails.
533723	In Linux, the default FTP client cannot fetch data using the proxy FTP over SSL.
533984	When using explicit web proxy, IP-address-based authentication fails.
535090	The FortiProxy unit fails to log in to the FTP server when using FTP explicit proxy.

Common vulnerabilities and exposures

FortiProxy 1.0.6 is no longer vulnerable to the following CVEs:

- CVE-2018-15473

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

Known issues

FortiProxy 1.0.6 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.