FortiProxy Release Notes

Version 1.0.4

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 31, 2018

FortiProxy 1.0.4 Release Notes

Revision 1

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Security modules 5
Caching and WAN optimization 5
What's new 6
Supported models 7
Product integration and support **8**
Web browser support 8
Fortinet product support 8
Virtualization environment support 8
Resolved issues **9**
Known issues **10**

Change log

Date	Change Description
August 31, 2018	Initial release for FortiProxy 1.0.4

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:

- Forced proxy. Using forced proxy in a firewall policy will proxy all TCP traffic in that policy, even if other features (such as UTM and web cache) are disabled. See the example.
- FQDN pattern matching. You can use `#` to indicate 0-9, `##` to indicate 00-99, and `###` to indicate 000-999 within the range defined by `pattern-start` and `pattern-end`. The `#` pattern can be in any position in the FQDN. For example, `a##b-c.dfg.com`, `##ab-c.dfg.com`, and `ab-c##` are valid; `a#b#c.dfg.cmo` is not valid. Using `###.push.apple.com` matches addresses from `001.push.apple.com` to `200.push.apple.com` in the example.

For example, if you want to use both FQDN pattern matching and forced proxy:

1. Create a firewall address, specifying the `fqdn-group` type, the pattern to match for the FQDN, and values for `pattern-start` and `pattern-end`.

```
config firewall address
   edit fqdn-grp1
      set type fqdn-group
      set fqdn ###.push.apple.com
      set pattern-start 001
      set pattern-end 200
      set cache-ttl 100
   end
```

2. Create a firewall policy using the firewall address that you created and specify forced proxy.

```
config firewall policy
   edit 1
      set service http
      set dstaddr fqdn-grp1
      set action accept
      set force-proxy enable
   end
```

Supported models

The following models are supported on FortiProxy 1.0.4, build 0050:

- 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 1.0.4:

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

Bug ID	Description
449765, 507889, 508154, 508329, 508334, 508853, 510131	Some GUI controls do not work as expected.
503667	The WAN optimization daemon (WAD) process crashes multiple times, and the WAD counter in the crash log is inaccurate.
504780	When a firewall policy is set to the “policy” type, the traffic log reports the policy type as “proxy-policy” instead of the “policy” type.
507188	When UTM is enabled, users cannot log in to a FortiProxy unit using an FTP server.
507557	When there is HTTPS traffic, the value for the Hit Count field is increased by 2 instead of by 1.
508112	For VM disks, the first disk is used for both WAN optimization and logging. The first disk should be reserved for logging.
508699	If a remote server is shut down when data is being uploaded, the data is queued inside of the FortiProxy unit instead of the session being closed.
508818	When using Chrome or Firefox and agentless NTLM, explicit proxy accepts empty credentials and then returns a 403 error.
510867	When the reverse-cache-prefetch configuration is enabled, the FortiProxy unit sometimes crashes instead of starting.

Known issues

FortiProxy 1.0.4 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.