FortiProxy Release Notes

Version 1.1.5

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

October 22, 2019

FortiProxy 1.1.5 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
October 22, 2019	Initial release for FortiProxy 1.1.5

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

FortiProxy version 1.1.5, build 0181, is a patch release only. There are no new features and enhancements in this release. For more information, see Resolved issues on page 9 and Known issues on page 11.

Supported models

The following models are supported on FortiProxy 1.1.5, build 0181:

- 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 1.1.5:

- 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

NOTE: Fortinet recommends running the FortiProxy VM with 2G+ memory because the AI-based Image Analyzer uses more memory comparing to the previous version.

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

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 1.1.5 or later is 2G. You must have at least 2G of memory to allocate to the FortiProxy VM from the VM host.

Upgrading the FortiProxy VM

If you are upgrading from FortiProxy 1.1.2 or earlier, including FortiProxy 1.0 to FortiProxy 1.1.5 or later, use the following procedure:

1. Back up the configuration from the GUI or CLI. Make sure the VM license file is stored on the PC or FTP or TFTP server.
2. Shut down the original VM.
3. Deploy the new VM. Make sure that there is at least 2G of memory to allocate to the VM.

4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI
6. Restore the configuration using the CLI or GUI.

Downgrading the FortiProxy VM

If you are downgrading from FortiProxy 1.1.5 or later to FortiProxy 1.1.2 or earlier, use the following procedure:

1. Back up the configuration from the GUI or CLI. Make sure the VM license file is stored on the PC or FTP or TFTP server.
2. Shut down the original VM.
3. Deploy the new VM. Make sure that there is at least 2G of memory to allocate to the VM.
4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI
6. Restore the configuration using the CLI or GUI.

Resolved issues

The following issues have been fixed in FortiProxy 1.1.5. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
471243	UTM logs do not report the “Subject,” “Recipient,” and “Sender” fields for emails sent using “MAPI over HTTPS.”
474239	Some DCE/RPC-mapped connections are intermittently blocked by policy 0.
511839	DLP sensors configured to block MAPI content (such as regexp, SSN, and credit card #) in email messages incorrectly log the filter category.
519874	When there are multiple violating attachments sent with the MAPI protocol, the email and all the attachments are blocked; however, not all attached files are logged as blocked.
538608	When the source interface is not configured in a link monitor entry or configured with an interface that does not match the gateway, the monitor route entry cannot be added.
540317	DLP cannot detect zip files attached to emails when receiving emails using MAPI over HTTP.
551956	Proxy web filtering blocks sites that were not in the block list for a few minutes to a few hours and then stops.
554664	The FortiView > Web Sites page is always blank.
554713, 554717	When you go to FortiView > Applications and drill down into countries, the window is blank.
567796, 585494, 587408, 589940	The WAN-optimization daemon (WAD) crashes.
572827	FTPS fails to log in to the server when using a transparent policy with UTM and certificate inspection enabled.
573971	FortiProxy should use the SSH session for SSH policy matching, instead of the HTTP explicit proxy session.
574191	The WAN optimization client side crashes when handling FTP get in active mode.
576274	When two FortiProxy units are in active-passive mode, the backup device responds to ARP requests and causes the network to go down.
576506	The Web Filter, Application Control, AntiVirus, and IPS logs to not show the user group.

Bug ID	Description
575264, 574447, 582124, 588868, 587989, 588173, 588667, 588868, 588988, 589396, 589433, 589970, 590207, 590211, 590226	Various features of the FortiProxy GUI need to be fixed or improved.
577242	When the disclaimer and deep inspection are enabled, web sites returned as the result of a Google search cannot viewed correctly.
579690	The `set replacemsg-override-group` command is not working in the firewall policy.
582124	The measurement units used in the Forward Traffic Logs and HTTP Transaction Logs should be consistent.
582783	The FortiProxy internal interface port2 does not reply to the SSL VPN client ping request.
584709	CLI and API input needs to be sanitized.
586210	When the source interface is a list of multiple interfaces, the authentication rule fails to match.
587165	The FQDN address match in the firewall policy fails after a configuration change.
587476	The authenticated user never expires after the SSH session exits.
588175	The email filter logs Outlook service messages as emails.
589882	The MAPI DLP log in FortiProxy shows the wrong filter category.
589962	Wildcard FQDN addresses need to be hidden in the source address list in the PAC policy.

Known issues

FortiProxy 1.1.5 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.