FortiProxy Release Notes

Version 1.2.0

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 16, 2019

FortiProxy 1.2.0 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
October 16, 2019	Initial release for FortiProxy 1.2.0

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:

- You can now specify thresholds for various Content Analysis categories in the GUI and CLI.
- An ICAP server is now supported with or without SSL encrypted configuration.
- The “Allow: 204” header and SSL encryption are now supported in the ICAP remote server configuration.
- You can ignore `robots.txt` rules when creating prefetch URLs and reverse cache prefetch URLs.
- You can now configure a user agent (such as Wget) for preloading URLs.
- The CIFS proxy solution has been enhanced.
- When you configure the authentication scheme (with the `config authentication scheme` command), you can enable extracting user information from the HTTP header (`set method x-auth-user`).
- There is now a dedicated management interface in NAT mode.
- A new CLI option (`set logic-type`) allows you to specify whether OR or AND logic is used for matching memberships of a user group.
- You can now specify multiple source interfaces with configuring authentication rules (with the `config authentication rule` command).
- The LDAP directory searching scalability has been improved by caching the LDAP/AD group and group-ID mapping and load-balancing to multiple ICAP servers through FQDN (with the `set ldap-user-cache` command).
- There are two new FortiView consoles: Link Monitor and FortiGuard Quota.
- You can now configure software-defined network (SDN) connectors (*System* > *SDN Connectors*).
- You can now configure isolator servers (*Policy & Objects* > *Isolator Server*).
- A new virtual machine is available to run on Microsoft Azure.
- You can now specify users and user groups as matching criteria in a traffic-shaping policy.

- User logout/override interface through the captive portal is now supported.
- The URL filter quota enforcement and management have been improved.
- UTM scan on SSH-tunneled TCP/IP traffic and SCP/SFTP is now supported.
- There are new CLI commands for displaying statistics:
    - `diagnose wad stats webproxy list`
    - `diagnose wad stats webproxy clear <webproxy-name>`
    - `diagnose wad stats sshproxy list`
    - `diagnose wad stats sshproxy clear`

Supported models

The following models are supported on FortiProxy 1.2.0, build 0274:

- 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 1.2.0:

- 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 1.2.9 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 1.2.0 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 1.2.0 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 1.2.0. 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.
490193	When the WAN optimization mode is changed in the CLI, the user should be prompted to confirm this action.
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.
527912	When a password on FortiCloud is longer than 20 characters, the user cannot connect to FortiProxy.
540317	DLP cannot detect zip files attached to emails when receiving emails using MAPI over HTTP.
541452	When the FortiProxy unit is using FTP proxy and matches a transparent policy with UTM enabled, the USER command is dropped.
543794	After upgrading to FortiProxy 6.0.4, the CPU runs at 100% because of the WAD process.
547426, 555421, 567796, 565143, 566964, 574256	The WAN-optimization daemon (WAD) crashes.
548487	When the FTP proxy is enabled and FTP traffic is generated from an avalanche, the console output is filled with multiple space.
553197	Synchronizing the configuration should exclude the x-cache-message.
554002	When preloading the reverse cache URLs, the interval needs to be more frequent.
551956	Proxy web filtering blocks sites that were not in the block list for a few minutes to a few hours and then stops.
554681	After importing a CA certificate, the “fnbamd” needs to be restarted before the CA certificate is used for verification.

Bug ID	Description
554713	When you go to *FortiView> Applications* and drill down into countries, the window is blank.
554874, 555689, 556792, 556812, 557103, 557722, 558258, 558337, 559144, 561379, 572560, 573080, 573083, 574157, 574447, 574774, 575264, 579012, 581302, 582124, 585213, 585479, 585764, 585849, 586183, 587989, 588136, 588138, 588173, 588203, 588868, 588928, 588988, 589396	Various features of the FortiProxy GUI need to be fixed or improved.
555061	The user information should be retrieved for SSH-tunnel policy matching.
556741	The VMware OVF file should have 2G memory by default.
557229	DNS protection should work even without any security profile applied to the policy.
557236	The logs should list DNS traffic as using the correct policy ID, instead of policy 0.
563749	Users of new FortiProxy units should be forced to change the administrator password when logging in to the CLI.
564397	The source and destination addresses of the shaping policy should filter out FQDN-wildcard addresses.
565206	After a successful preload, the result of the `execute preload show-log` command is always empty.
569190	Loading the `FortiProxy-VM64.hw07_vmxnet3.ovf` file causes the following error: `__get_mtner_timerout: Couldn't get shm(please refer to attachment)`
572834	The redirect feature in the policy does not work.
576718	The FTP status code produced by the firewall is inconsistent when there is a passive connection and when there is an active connection.
577242	When the disclaimer and deep inspection are enabled, web sites returned as the result of a Google search cannot viewed correctly.

Bug ID	Description
582124	The measurement units used in the Forward Traffic Logs and HTTP Transaction Logs should be consistent.
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.
579690	The `set replacemsg-override-group` command is not working in the firewall policy.
582297	No traffic logs are generated by UTM scan for antivirus, web filter and DLP in the SSH-tunnel policy.
587194	The ICAP CLI commands need to be reorganized.
588206	There are missing fields for the web-proxy pac-policy CLI.

Common vulnerabilities and exposures

FortiProxy 1.2.0 is no longer vulnerable to the following CVEs:

- CVE-2019-11477
- CVE-2019-11478
- CVE-2017-17544

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

Known issues

FortiProxy 1.2.0 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.