FortiProxy Release Notes

Version 1.1.4

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

July 30, 2019

FortiProxy 1.1.4 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
July 30, 2019	Initial release for FortiProxy 1.1.4

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.
- **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:

- A new virtual machine is available that runs on the Microsoft Azure cloud.
- FortiProxy now uses the HTTP “x-authenticated-user” header for LDAP user authorization. Use the following commands to enable this feature:

```
config authentication scheme
  edit <authentication_scheme_name>
     set method x-auth-user
  end
```

Supported models

The following models are supported on FortiProxy 1.1.4, build 0175:

- 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 1.1.4:

- 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

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 1.1.4 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 1.1.4 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 1.1.4 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 1.1.4. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
527912	When a password on FortiCloud is longer than 20 characters, users cannot access FortiProxy.
541452	Logging in with FTP proxy might fail when using a transparent policy with UTM enabled.
543794	WAN-optimization daemon (WAD) process causes the CPU usage to be 100%.
548487	Multiple spaces appear in the console output when generating FTP traffic.
555395	When connecting to an FTPS server from an FTP client, logging in fails because the wrong authentication rule is matched.
559144	You cannot change the value of the Class ID field of an existing traffic shaper.
560224	The TLS fingerprint library needs to be updated.
560280	There are issues connecting with FortiManager.
561163	The FortiProxy VM crashes when it is deployed on the Microsoft Azure cloud.
561957	After upgrading, prefetch entries are missing in the in reverse-cache-server configuration.
564397	When the source or destination address is defined in a firewall shaping policy, the FQDN wildcard type addresses should be filtered.
565143	There are frequent WAD process crashes.
565762	The FortiProxy instance is not reading the user data configured on the AWS cloud.
566964	FortiProxy stopped responding because of a buffer issue.
569190	An error occurs when deploying the FortiProxy VM (VMware) on ESXi 6.5 Update B2 and VM Workstation version 8.
570640	When web caching for HTTPS traffic is enabled, Live YouTube Stream stops after approximately 20 seconds.
570886	When the arp-max-entry value is set to 131072, the value of 1024 is used instead.
571369	WAD sessions remain open after kernel sessions are closed.
572834	Redirecting some source IP addresses or users to a web site causes a WAD application crash.

Bug ID	Description
572851	The table sizes in the configuration file should change according to the VM license.
573080	The traffic shaper profile should not be created when the bandwidth value in the class is invalid.
573083	When creating or editing a traffic shaper, the user should be able to set the Default Class field to 1. Also, when creating or editing a traffic shaping policy, the user should be able to set the Class ID field to 1.
573486	Web filter logs do not appear in the FortiProxy GUI.

Common vulnerabilities and exposures

FortiProxy 1.1.4 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 1.1.4 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.