FortiProxy Release Notes

Version 2.0.0

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

February 23, 2021

FortiProxy 2.0.0 Release Notes

Revision 4

TABLE OF CONTENTS

Change log

Date	Change Description
November 13, 2020	Initial release for FortiProxy 2.0.0
November 16, 2020	Updated the “Virtualization environment support” section.
December 2, 2020	Updated the “What’s new” section. Added to the description of bug 491027.
February 23, 2021	Added the “Fortinet Single Sign-On (FSSO) support” section.

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:

- The number of sessions per seat has been increased from 10 sessions per seat to 25 sessions per seat.
- Port mirroring and SSL mirroring are now supported. This feature allows the FortiProxy unit to decrypt and mirror traffic to a designated port. A decrypted traffic mirror profile can be applied to explicit, transparent, SSH tunnel, and SSH proxy policies when the custom-deep-inspection, deep-inspection, or deep-test SSL/SSH inspection security profile is selected.
- FortiProxy High Availability (HA) can now synchronize configuration changes among 32 clustering members. The Cache Collaboration feature is also supported across the clustering members.
- The menus in the web UI have been reorganized to focus on proxy configuration and to make it easier to navigate.
- You can now create an administrator account for the FortiProxy REST API. (See the FortiProxy REST API documentation on https://fndn.fortinet.net.)
- Improved Content Analysis
  - You can now specify that an image is skipped for Content Analysis if the width or height are too small.
  - A new Gambling category has been added.
  - You can now choose one of three different policy states (Allow, Deny, and Monitor) for each content category.
- There are new options for the global explicit web proxy settings (*Proxy Settings* > *Web Proxy Setting*):
  - Fast Policy Match
  - LDAP User Cache
  - Strict Web Check
  - Forward Proxy Auth
  - Non HTTP Traffic
- There are new options for the antivirus security profile (*Security Profiles* > *AntiVirus*)
  - File quarantine
  - Archive block
  - Archive log
  - Send files to FortiSandbox Cloud for inspection
  - Use FortiSandbox database

Supported models

The following models are supported on FortiProxy 2.0.0, build 0012:

FortiProxy	• FPX-2000E • FPX-4000E • FPX-400E

FortiProxy VM	• FPX-AZURE • FPX-HY • FPX-KVM • FPX-KVM-AWS • FPX-KVM-GCP • FPX-KVM-OPC • FPX-VMWARE

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 2.0.0:

- 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

Software upgrade path

FortiProxy supports upgrading directly from 1.0.x, 1.1.x, or 1.2.x to 2.0.0.

Fortinet Single Sign-On (FSSO) support

- 5.0 build 0295 and later (needed for FSSO agent support OU in group filters)
    - Windows Server 2019 Standard
    - Windows Server 2019 Datacenter
    - Windows Server 2019 Core
    - Windows Server 2016 Datacenter
    - Windows Server 2016 Standard
    - Windows Server 2016 Core
    - Windows Server 2012 Standard
    - Windows Server 2012 R2 Standard
    - Windows Server 2012 Core
    - Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
    - Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
    - Windows Server 2008 Core (requires Microsoft SHA2 support package)
    - Novell eDirectory 8.8

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, 6.5, and 6.7
HyperV	• Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 2.0.0 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 2.0.0 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 2.0.0 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 issue has been fixed in FortiProxy 2.0.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
586764	When modifying a large policy list, there is an abnormal prolonged CPU usage increase.
604699	Adding an extra space to the HOST header causes a memory leak.
619707	The WAD is causing high memory usage when using explicit proxy with more than 30 users.
630433	Instead of using the `set category-override` command under `config webfilter profile`, you can now control which categories are used by specifying them with the `set category` command under `edit filters`.
637596	The web filter blocks traffic when using the proxy policy.
639086	Stale WAD users cannot be removed from the table.
640488, 645943	The memory usage for all WAD instances increases for about 60 seconds periodically.
647227	When an external list has been imported as a remote category that is blocked, the domain name in the web filter is incorrectly matched.
651314	There are multiple fnbamd crashes when a Config-Sync cluster was configured with LDAP authentication and load balancing.
654106	When editing the LDAP server entry, the port resets back to 636.
654279	The life traffic analysis in FortiView did not show any activity details.
654539	The active authentication scheme is not applied as the default authentication scheme.
654684	The WAD process continuously crashes with a signal 6 (Aborted) received on a FortiProxy-4000E unit.
655754	The FortiProxy VM has high memory usage when there is no traffic, and the dnsproxy daemon is being killed frequently.
657563	When the FortiProxy unit is configured as a WCCP client, redirected traffic is being dropped when web caching is enabled in the policy.
661695	The WAD continuously crashes on a FortiProxy 4000E unit.
670528	Changing the setting for a Content Analysis category still allows images that should be blocked.

Bug ID	Description
675473	The local ICAP server does not block viruses as configured.
677158	The DLP file name pattern cannot be added in the GUI.

Known issues

FortiProxy 2.0.0 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. **Workaround:** The fix is scheduled for a future release.
490951	The `append explicit-outgoing-ip` command is not validated.
499787	The FortiGuard firmware versions are not listed on the *System* > *Firmware* page.