FortiProxy Release Notes

Version 2.0.4

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

June 1, 2021

FortiProxy 2.0.4 Release Notes

Revision 2

TABLE OF CONTENTS

Change log

Date	Change Description
April 23, 2021	Initial release for FortiProxy 2.0.4
June 1, 2021	Updated the “Common vulnerabilities and exposures” 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.

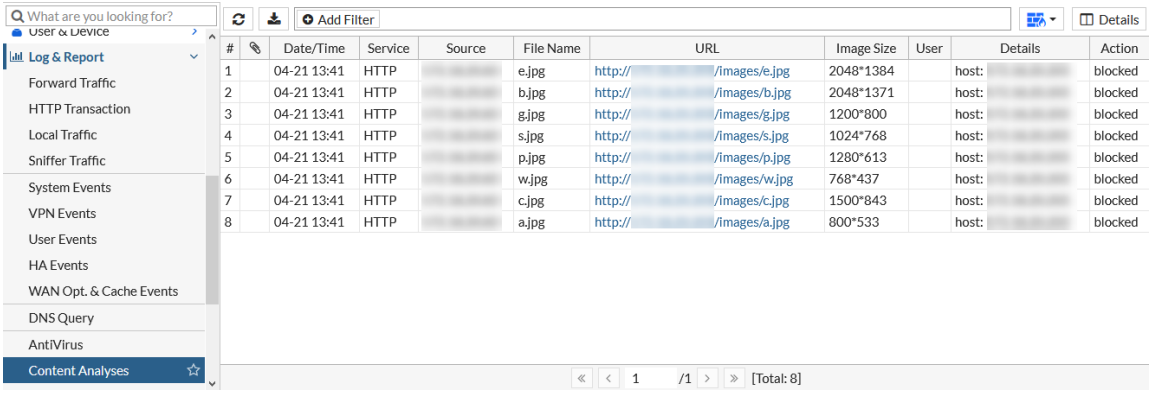
FortiProxy is intelligent enough to understand the differing caching formats of the major video services in order to maximize cache rates for one of the biggest contributors to bandwidth usage. FortiProxy will:

- 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 table size for proxy addresses has been increased from 8,000 entries to approximately 24,000 entries.
- Configuring the `set ipv4-trusthost` command (under `config system api-user`) is no longer mandatory, and the default value is null.
- You can now review content-analysis events by going to *Log & Report* > *Content Analyses*.



The Content Analyses log contains the following fields by default:

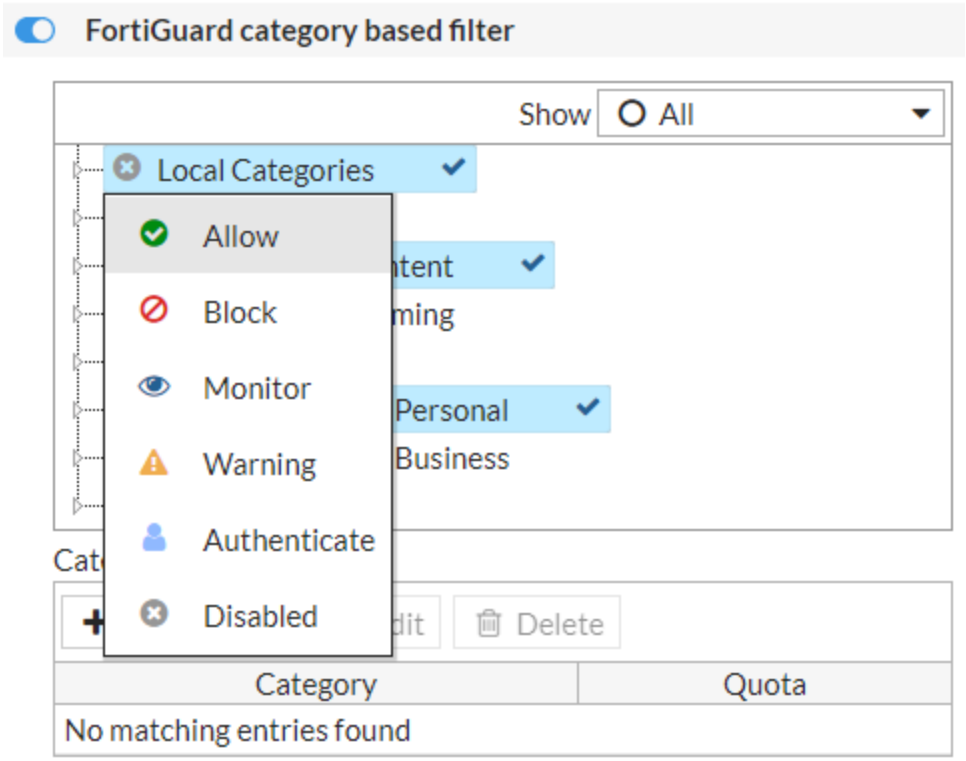
- #—Log identifier
- Attachment—Whether there was an attachment.
- Date/Time—Day, month, year, and time when the log event occurred.
- Service—Name of the service.
- Source—IP address of the traffic's origin.
- File name—The image.
- URL—Where the image is saved.
- Image Size—How large the image is.
- User—The user who viewed the image.
- Details—The host where the image was viewed.
- Action—Status of the session.

The following columns are also available:

- Agent
- Checksum
- Command
- Destination
- Destination Interface
- Destination Interface Role
- Destination Port
- Detection Type
- Direction
- Event Type
- File Filter Type
- File Type
- FortiClient ID

    - FortiSandbox Checksum
    - FortiSandbox Verdict
    - From
    - Group
    - Level
    - Log ID
    - Log event original timestamp
    - Message
    - New Protocol
    - Policy
    - Profile Name
    - Protocol
    - Quarantine Skip
    - Recipient
    - Reference
    - Sender
    - Session ID
    - Source Interface
    - Source Interface Role
    - Source Port
    - Sub Service
    - Submitted to FortiSandbox
    - Threat Level
    - Threat Score
    - Timestamp
    - To
    - True-Client-IP Header
    - Type
    - Unauthenticated User
    - Unauthenticated User Source
    - Violate Category
    - Violate Score
    - Virus ID
    - Virus/Botnet
    - X-Forwarded-For Header
    - scorelist
- Previously, setting a custom category to *Allow* in a web filter profile in the FortiProxy GUI caused the web filter category override to not work; this issue has been fixed. In addition, creating or editing a filter in the web filter profile in the GUI has been improved:
    - The default action for a category under Local Categories or Remote Categories is *Disabled*, which removes the configuration in the CLI.
    - When a category under Local Categories or Remote Categories is not configured in the web filter profile, the category is shown as *Disabled*.
    - When a category under Local Categories or Remote Categories has the action set to Monitor and logging disabled, the category is shown as *Allow*.

- When a category under Local Categories or Remote Categories has the action set to Monitor and logging enabled, the category is shown as *Monitor*.
- Right-clicking on Local Categories or Remote Categories displays the following choices:



- You can now use RAPTOR syntax when providing ftp-user, ftp-dest, and proxy-user to FortiProxy for explicit FTP proxy. For example: `USER ftp-user@ftp-dest proxy-user`

  The syntax is identified automatically without any changes in the CLI configuration.

  NOTE: You need to configure an authentication scheme and an authentication rule to use firewall authentication.

Supported models

The following models are supported on FortiProxy 2.0.4, build 0039:

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 • FPX-XEN

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 2.0.4:

- 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

Software upgrade path

FortiProxy supports upgrading directly from 1.0.x, 1.1.x, or 1.2.x to 2.0.4.

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.

HyperV	• Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Xen hypervisor	• OpenXen 4.13 hypervisor and later • Citrix Hypervisor 7 and later
VMware	• ESXi versions 6.0, 6.5, 6.7, and 7.0

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 2.0.4 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 2.0.4 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 2.0.4 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 2.0.4. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
594580	When using FTP over HTTP, no traffic logs are generated if an error 500 is received while navigating through the FTP directory.
633108	Shutting down from the HTTP client port causes the WAN-optimization daemon (WAD) process to crash.
633974	No replacement message is provided when an oversized file is detected with an FTP-over-HTTP proxy policy.
692444	WAD memory usage increases until conserve mode is reached.
702298	PDF files are not blocked when using `filter-by credit-card` and `filter-by regexp` configured in the DLP sensor.
704877	The ICAP server is not blocking files when using a DLP sensor with `filter-by file-type` configured.
706974	There should be a warning if the captive portal is not enabled when it is needed for the SAML authentication method.
707087	A memory leak occurred when the HTTP transaction log was enabled.
707560	Policies that use the proxy address object cause a warning message and cannot be saved after changes to the policies.
707689	A programming tool found an invalid read of memory when testing transparent proxy authentication.
709926	The output for the `diagnose wad license summary` command shows the wrong number of users and sessions.
711409	When `config user ldap` is set up, the CPU spins.
712217	Setting the FortiGuard category-based filter to “warning” or “authenticate” does not work.
712701	The FortiProxy unit will restart when the firewall policy is disabled while traffic is flowing.
713347	The ICAP server does not support IPv6 addresses.
713400	The ICAP secure connection failed between the FortiProxy unit’s ICAP client and server.
713538	When a user is configuring the explicit FTP-proxy rule, the warning to enable explicit proxy refers to the wrong menu command.

Bug ID	Description
713646	The reason for authentication failing needs to be clearer when explicit FTP proxy is configured with authentication on a policy but missing the authentication rule.

Common vulnerabilities and exposures

FortiProxy 2.0.4 is no longer vulnerable to the following CVEs:

- CVE-2020-12812
- CWE-295
- CWE-352

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

Known issues

FortiProxy 2.0.4 includes the known issues listed in this section. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
491027, 681567	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.

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.