FortiProxy Release Notes

Version 2.0.8

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

March 9, 2022

FortiProxy 2.0.8 Release Notes

Revision 2

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Security modules 5
Caching and WAN optimization 6
What's new 7
Implicit enforcement of deep inspection for user friendly policy matching 7
Limiting the access of nondomain users 7
Disabling IP-based URL rating 7
New diagnose command 8
Supported models 9
Product integration and support **10**
Web browser support 10
Fortinet product support 10
Software upgrade path 10
Fortinet Single Sign-On (FSSO) support 10
Virtualization environment support 11
New deployment of the FortiProxy VM 11
Upgrading the FortiProxy VM 11
Downgrading the FortiProxy VM 11
Resolved issues **13**
Common vulnerabilities and exposures 14
Known issues **15**

Change log

Date	Change Description
February 18, 2022	Initial release for FortiProxy 2.0.8
March 9, 2022	Updated the “Disabling IP-based URL rating” 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.

Implicit enforcement of deep inspection for user friendly policy matching

When the HTTP CONNECT request or the Transport Layer Security (TLS) server name indication (SNI) partially matches a policy with deep inspection is enabled, deep inspection of the policy is enforced with the HTTPS traffic.

Limiting the access of nondomain users

You can now limit the access of nondomain users while using proxy authentication. To do so:

- Use the negotiate authentication scheme.
- Disable NTLM negotiation.

For example:

```
config authentication scheme
   edit "negotiateonly"
      set method negotiate
      set negotiate-ntlm disable
      set kerberos-keytab "fpx45.dev.fgt.com"
   next
end
config authentication rule
   edit "negotiaterule"
      set srcaddr "all"
      set dstaddr "all"
      set srcaddr6 "all"
      set active-auth-method "negotiateonly"
   next
end
```

Disabling IP-based URL rating

You can now disable IP-based URL rating for SSL-exemption and proxy-address objects. By default, IP-based URL rating is enabled. Use the following CLI commands:

```
config firewall ssl-ssh-profile
   edit <name>
      set ssl-exemption-ip-rating {enable | disable}
   next
end
config firewall profile-protocol-options
   edit <name>
   config http
      set address-ip-rating {enable | disable}
   next
end
```

New diagnose command

The new `diagnose wad user count` command displays the number of active, anonymous, and stale users of each WAD worker.

Supported models

The following models are supported on FortiProxy 2.0.8, build 0078:

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 2.0.8:

- 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 2.0.8.

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 2.0.8 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 2.0.8 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

Do not downgrade the FortiProxy 2.0.6 VM because the new VM license file cannot be used by earlier versions of FortiProxy.

If you are downgrading from FortiProxy 2.0.5 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 2.0.8. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
746009	The IP pool configuration in an explicit policy is ignored on outbound traffic.
753952	The FortiProxy GUI does not allow the SSL/SSH inspection profile to be set in an ISDB deny policy.
757800	When using IP-based Kerberos authentication, FortiView displays the number of bytes but not the user group or authentication type.
761568	The WAN-optimization daemon (WAD) crashes multiple times after the user upgrades from FortiProxy 2.0.6 to 7.0.1.
763977	The DLP filter wrongly identifies PDF files as executables.
764462	Administrative Telnet access automatically enables on ha-mgmt-interfaces.
764990	Upgrading the firmware of a FortiProxy unit that is a member of an HA Config-Sync cluster causes a wa_cs crash.
767401	Client-side WAN optimization results in the WAD crashing.
768699	The WAD crashes if the authentication rule configuration is updated while the WAD is synchronizing.
768980	The Host Regex feature is not working correctly.
769966	When FortiProxy is configured for explicit proxy and Config-Sync mode, the WAD uses 99 percent of the CPU until the WAD process is restarted.
769970	The HTTP GET URL value is missing in FortiProxy 2.0.7 when using the web proxy with the forwarding server.
770178	When a proxy address is used as the destination in a policy, unrelated traffic matches the policy.
771142	After the WAN-optimization configuration is changed, the WAD process crashes.
773704	Client comfort is not applied to HTTPS traffic when deep inspection is enabled.
775626	Upgrading the firmware in an HA Config-Sync cluster fails.
775648	The forward traffic logs do not display the FSSO user names.
775865	When the FortiProxy unit is using form-based authentication, a 404 error occurs.

Bug ID	Description
777082	When the FortiProxy unit is in transparent mode, NTLM authentication does not work.
777344	A WAD memory leak occurs when using ICAP.
777370	When fast-match is disabled, the HTTPS request fails to match the source proxy address in the policy.
777718	The WAD should use the port in the TCP header to match the service field.
777905	The response for the HTTPS request includes two “Transfer-Encoding: chunked” lines.
779277	Explicit proxy should be able to authenticate with the HTTP CONNECT method and respond with the 407 response code.
779468	Should not send a 401 response to HTTPS CONNECT request when user authentication is enabled in a transparent firewall policy.
781096	When the `ha-direct` setting is enabled, RADIUS requests still use the default route.
781308	HTTPS traffic to the ZTNA server is blocked.
781900	When the HTTP Authorization request header contains an existing FortiProxy user, IPS might reset, and the request fails.
783235	Deep scanning does not work when the transparent proxy policy has the proxy address and deep inspection enabled and there is another transparent proxy policy with a proxy address and certificate inspection.
783348	The ssh-filter-profile specified in the policy is not used when authentication is required.
783436	The ICAP client crashes because of a memory leak.

Common vulnerabilities and exposures

FortiProxy 2.0.8 is no longer vulnerable to the following CVEs:

- CWE-79
- CWE-120
- CWE-121
- CWE-124
- CWE-134
- CWE-190
- CWE-347

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

Known issues

FortiProxy 2.0.8 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:**Upgrade to FortiProxy 7.0.0.
490951	The `append explicit-outgoing-ip` command is not validated.
499787	The FortiGuard firmware versions are not listed on the *System* > *Firmware* page.