FortiProxy Release Notes

Version 2.0.1

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 2.0.1 Release Notes

Revision 2

TABLE OF CONTENTS

Change log

Date	Change Description
December 21, 2020	Initial release for FortiProxy 2.0.1
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:

- You can now configure a SAML 2.0 server for authentication with FortiProxy as the service provider (SP) . To use the GUI, go to *User & Device* > *SAML* and select *Create New*. The following are the CLI commands:

```
config user saml
   edit <SAML_server_entry_name>
      set cert <certificate_to_sign_SAML_messages>
      set entity-id <service_provider_entity_ID>
      set single-sign-on-url <service_provider_single_sign-on_URL>
      set single-logout-url <service_provider_single_logout_URL>
      set idp-entity-id <identity_provider_entity_ID>
      set idp-single-sign-on-url <identity_provider_single_sign-on_URL>
      set idp-single-logout-url <identity_provider_single_logout_URL>
      set idp-cert <identity_provider_certificate_name>
      set user-name <user_name_in_assertion_statement>
      set group-name <group_name_in_assertion_statement>
      set algo {sha1 | sh256}
      set adfs-claim {enable | disable}
      set user-claim-type {email | given-name | name | upn | common-name |
          email-adfs-1x | group | upn-adfs-1x | role | sur-name | ppid |
          name-identifier | authentication-method | deny-only-group-sid |
          deny-only-primary-sid | deny-only-primary-group-sid | group-sid |
          primary-group-sid | primary-sid | windows-account-name }
      set group-claim-type {email | given-name | name | upn | common-name |
          email-adfs-1x | group | upn-adfs-1x | role | sur-name | ppid |
          name-identifier | authentication-method | deny-only-group-sid |
          deny-only-primary-sid | deny-only-primary-group-sid | group-sid |
          primary-group-sid | primary-sid | windows-account-name }
   next
end
```

- You can now configure an authentication scheme for a SAML 2.0 server with FortiProxy as the SP. To use the GUI, go to *Policy & Objects* > *Authentication Rules*, select *Create New* > *Authentication Schemes*, and then select the SAML-SP method. The following are the CLI commands:

```
config authentication scheme
   edit <authentication_scheme_name>
      set method saml-sp
      set saml-server <SAML_configuration>
      set saml-timeout <30-1200 seconds>
      set user-database <authentication_server_name>
   next
end
```

- You can now configure an IP address for the captive portal. To use the GUI, go to *Policy & Objects* > *Proxy Auth Setting*, select *IP* for the *Captive Portal Type* setting, and then enter the IPv4 address. The following are the CLI commands:

```
config authentication setting
   set captive-portal-type ip
   set captive-poral-ip <xxx.xxx.xxx.xxx>
end
```

- You can now back up the FortiProxy configuration to a SSH File Transfer Protocol (SFTP) server. Use the following CLI command:

```
execute backup config <destination_IP_address> <SFTP_server_user_name>
    <SFTP_server_password> <destination_file_path> [<optional_password_for_
    backup_file>]
```

- You can now create a data loss prevention (DLP) sensor with a filter to block files of a specific file type that also exceed a specified file size. Use the following CLI commands:

```
config dlp sensor
   edit <name>
      set comment <comment>
      set replacemsg-group <string>
      set dlp-log {enable | disable}
      set nac-quar-log {enable | disable}
      set summary-proto {smtp | pop3 | imap | http-get | http-post | ftp |
          nntp | mapi | cifs | ssh}
      config filter
         edit <id>
            set name <filter_name>
            set severity {info | low | medium | high | critical}
            set type {file | message}
            set proto {smtp | pop3 | imap | http-get | http-post | ftp | nntp
                | mapi | cifs | ssh}
            set filter-by {credit-card | ssn | regexp | file-type | file-size
                | watermark | encrypted | file-type-and-size}
            set file-size <0-4294967295 kbytes>
            set file-type {builtin-patterns | all_executables}
            set action {allow | log-only | block | quarantine-ip}
         next
      end
   next
end
```

Supported models

The following models are supported on FortiProxy 2.0.1, build 0018:

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 2.0.1:

- 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 2.0.1.

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 2.0.1 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 2.0.1 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 2.0.1 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 2.0.1. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
609568	When using MAPI over HTTP (Active-Passive) mode, the WAN-optimization tunnels are sometimes not established.
635346	The `set return-to-sender enable` command causes the FortiProxy unit to reboot, resulting in disk corruption.
669878	Running the `exec report run` CLI command causes the report daemon to crash.
670917	An IPsec tunnel cannot be brought up the first time after creating or modifying it.
671803	When a policy has a configured proxy address, SSH and FTP traffic is not accepted.
676516	The active method in the authentication rule should not select the header type scheme.
677305	When `logtraffic-start` is enabled, the start of the SSH session is not being logged.
677393	The CLI need to support the changes in specific commands to eliminate references to “slave” and “master.”
677606	When the policy type is explicit FTP, the web cache and web proxy profile should be hidden.
677683	The WAD process crashes when no ICAP service is mapped.
677743	The local ICAP server has memory corruptions.
677843	The WAN-optimization daemon (WAD) process is causing high memory usage, and the wa_cs process is crashing.
678157	A new antivirus profile cannot be created or edited in the GUI.
678746	When applying log settings, the confirmation page is displayed twice.
680892	The DLP system is not blocking files according to the configured file type.
681017	The Security Fabric widget in the FortiProxy dashboard should display the correct IP address.
681250	Configuring HA in the GUI causes the HTTPS daemon to crash.
681461	When incoming-ip is set for explicit FTP proxy, iptables ignores it.
681677	A programming tool discovered an invalid read/write.

Bug ID	Description
682254	When deploying a new FortiProxy VM on Azure, you can set the user name and password; however, you cannot log in to the VM with the user name and password that was configured.
682403	Favorites for *FortiView* > *Peer Monitor*, *FortiView* > *Optimization Monitor*, and FortiView > Cache Monitor are shown as “undefined” in the Favorites menu.
682419	Duplicate policy rules are created if the right-hand selection pane is displayed in the GUI and *OK* is selected.
682436	Saving policy rules results in an “Input value is invalid” message.
682615	Creating an explicit or transparent policy in the GUI results in a duplicate policy.
682618	Deleting one or more policy from the GUI results in multiple confirmation pages.
682827	Various issues with the ICAP server need to be fixed.
683238	Traffic-shaping profiles that use Application ID/Category are being ignored.
683833	The WAD process is causing high memory usage and is crashing.
684464	The captive portal port is not listening on FQDN addresses.
684510	There is an internal 500 error when trying to save SSL-VPN settings in the GUI.
684809	Updating the FortiProxy image causes the authentication scheme configuration to be lost.
684972	The WAD process crashes when the DLP sensor detects an oversized file.
685558	The `set pac-data enable` command cause the matched cached group to be “NA.”
609092	When the captive portal and matching the full URL with HTTPS are configured, the WAD process crashes.

Common vulnerabilities and exposures

FortiProxy 2.0.1 is no longer vulnerable to the following CVEs:

- CVE-2015-2267
- CVE-2018-13379
- CVE-2018-13380
- CVE-2018-13381
- CVE-2018-13382
- CVE-2018-13383
- CVE-2018-13384
- CVE-2019-15706
- CVE-2020-6648
- CWE-922

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

Known issues

FortiProxy 2.0.1 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.