FortiProxy Release Notes

Version 1.1.1

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 12, 2019

FortiProxy 1.1.1 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
February 12, 2019	Initial release for FortiProxy 1.1.1

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 maximum number of sessions per user is now 10. For example, for a 100-user license, 1,000 proxied sessions with UTM scan are allowed. A single source IP address can use all sessions if needed.
- Two new widgets that can be displayed on the *Dashboard > Main* page show the numbers of logged-in users and proxied sessions over intervals from 1 minute to 24 hours.
- You can now allow the explicit web proxy to return packets to the interface or MAC address of the original request instead of using the route information. To control this feature, use the following CLI commands:

```
config web-proxy explicit
   edit "name_of_explicit_web_proxy"
      set return-to-sender {enable | disable}
   next
end
```

- When you create a proxy policy for the CIPS protocol (SMB 3.0 and later), you can derive user authentication information from a replication user in the Active Directory. To control this feature, use the following CLI commands:

```
config cifs profile
   edit "name_of_CIFS_profile"
      set server-credential-type credential-replication
      set domain-controller "<network_service>"
   next
end
```

- If you enable dynamic sizing for the TCP window, the TCP window size will adjust, based on the available memory and user-specified maximum and minimum values. For example:

```
config firewall profile-protocol-options
   edit "default"
      config http
         set tcp-window-type system dynamic
         set tcp-window-minimum 131072
         set tcp-window-maximum 8388608
      end
   next
end
```

Supported models

The following models are supported on FortiProxy 1.1.1, build 0154:

- 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 1.1.1:

- 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

Virtualization environment support

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

Resolved issues

The following issues have been fixed in FortiProxy 1.1.1. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
460211	When there is a partial content response for an expired object, the WAN optimization daemon (WAD) returns an empty reply.
499496	SMTPS traffic containing an IPS attack should be dropped when the action is set to block it in the IPS sensor.
515468	When SSL Nego is in active mode, the response is “500 Illegal PORT command.”
517909	The `mget` command does not get the files from the FTP server through the WAN optimization tunnel.
519702	SSH deep inspection is not logging or blocking SFTP.
521344	The explicit FTP proxy does not work with a secondary IP address.
522441	Some live video sites were not being cached.
523204	The WAD stops responding, and there is a signal 11 (Segmentation fault) received.
524549	SSH should be disabled by default in certificate-inspection.
527467	VPN tunnels are not listed in the GUI.
527660	*Log > VPN Events* is empty when there should be log entries.
529553	FTP proxy failures need to be fixed.
529769	The source and destination interfaces cannot be set to “any.”
529999	The FortiGate unit blocks traffic successfully with “block-client-cert,” but the sslaction field in the FortiGate traffic log is inaccurate.
519702, 530127, 530990, 531608, 532461, 532540, 532785, 532918, 533931, 536102, 536862, 537543, 537564, 537572, 537966, 537991	The GUI features that do not work as expected need to be fixed.

Bug ID	Description
530669	When the explicit proxy and SD-WAN are enabled, matching traffic is not forwarded using the correct interface.
531116	FortiProxy caching collaboration is not working between two FortiProxy units in the Config-Sync (HA) mode.
531339	A wildcard FQDN object should not be able to be added in an address group in the CLI.
531377	The WAD stops responding when fast-policy-match is enabled.
531402	After entering memory conserve mode, the FortiProxy disks are disabled.
531526	The explicit FTP proxy ignores the use of a one-time password for authentication.
531575	A web site cannot be accessed when using a web proxy policy with deep SSL inspection.
532484	When the TLS connection is terminated, FortiProxy should generate a log message.
532758	WAN optimization with explicit proxy should not allow buffer overruns
532759, 532762, 532766	WAN optimization with explicit proxy should not allow large parameters to be passed by value.
532760, 532764	WAN optimization with explicit proxy should not allow time-of-check to time-of use race conditions.
532761, 532765	WAN optimization with explicit proxy should not allow the forwarding of null values.
532833	When upgrading from FortiProxy 1.0.5 to 1.1, error -56 is reported.
533089	When a source peer is changed, caching collaboration fails.
533671	WAD cannot handle the EPSV command.
533723	In Linux, the default FTP client cannot fetch data using the proxy FTP over SSL.
533931	When the source is changed from “any” to a peer, the caching cluster fails to work.
533984	IP-based authentication fails when using explicit proxy.
534346	A WAD memory leak occurs during OCSP certificate caching.
534529	UTM profiles should be able to be set even if the utm-status is disabled.
534580	Routes added by the link monitor should be identified as such.
534617	Routes added by the link monitor should not affect traffic routing.

Bug ID	Description
534942	There should be log entries when the license limit is exceeded.
535090	Users cannot log in to the FTP server when using FTP explicit proxy.
535204	The HD2 disk is disabled on the FortiProxy VM when using WAN optimization and logging in to the GUI.
535882	When using the agentless NTLM authentication method in the proxy policy, the locally defined LDAP-type user cannot be matched.
536063	Deep inspection in explicit proxy does not work for some websites.
536102	The FortiProxy GUI should allow wildcard-fqdn addresses and address groups that contain wildcard-fqdn addresses.
536370	A FortiGate unit with the inspect-all profile is not blocking untrusted and invalid certificates.
536623	IPS should be able to decrypt sessions even if other flow-based security profiles are present in the same policy.
536857	When the inbandwidth and outbandwidth values are specified for the WAN interface, LAN clients cannot connect to the Internet.
537183	When deep inspection blocks a page, there should be a message in the log.
537346	A disclaimer message should be displayed and acknowledged before the end user can browse the Internet.
538197	After a factory reset, the value for update-server-location is “usa.”

Known issues

FortiProxy 1.1.1 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.
490951	The `append explicit-outgoing-ip` command is not validated.
499787	The FortiGuard firmware versions are not listed on the *System* > *Firmware* page.