FortiProxy Release Notes

Version 1.1.3

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

May 17, 2019

FortiProxy 1.1.3 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
May 17, 2019	Initial release for FortiProxy 1.1.3

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 control the maximum number of sessions per user with the following commands:

```
config system global
   set max-session-per-user <number_of_sessions>
end
config firewall policy
   edit <policy_number>
      set max-session-per-user <number_of_sessions>
   end
```

  If `max-session-per-user` is not set at the policy level, the global setting is applied. If `max-session-per-user` is set at the policy level, the policy-level setting overrides the global setting.

- The Image Analyzer can now scan multiple categories.
- There are changes to deploying, upgrading, and downgrading FortiProxy VMs. See Virtualization environment support on page 8.
- The support for FortiIsolator has been improved. Use the following commands:

```
config firewall policy
   edit <policy_number>
      set action isolate
      set fortiisolator-server "<name_of_FortiIsolator_server>"
   next
end
```

  When the `action` is set to `isolate`, you must specify the `fortiisolator-server` setting. You cannot set both the `forward-server` and `fortiisolator-server`.

Supported models

The following models are supported on FortiProxy 1.1.3, build 0171:

- 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 1.1.3:

- 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

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, and 6.5

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 1.1.3 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 1.1.3 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 1.1.3 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 1.1.3. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
513470	Periodic WAN-optimization daemon (WAD) crashes are seen in the crash log.
541423	When using the ICAP profile and a max-connection value of 16, the ICAP server rejects connections (because of too many connections) after any change is applied over the FortiGate unit.
543447	When the ICAP profile is enabled in the policy, some Internet sites do not load.
547426	After upgrading from FortiOS 6.0.4 to 6.2, WAD crashes.
549874	When ICAP is enabled and antivirus scan is disabled, WAD crashes.
550726	After creating a new DNS filter and enabling the External IP Block List, there is an “Error 500: Internal Server Error” when saving.
551285	Using an DNS filter with Remote Categories and the action set to Monitor or Block causes an “Invalid category or group” message.
551337	Upgrading from 1.1.1 to 1.1.2 caused the reverse cache server configuration and prefetch URL configuration to return to the default configuration.
551523	The \domain\user format is not supported in the basic authentication.
551554	The license file generated by the latest version of licensegen is not working on the FortiProxy 1.0 VM.
552284	Using the External Resource IP type should not cause the CPU usage to rise to 100%.
553197	Synchronizing the configuration in a FortiProxy cluster causes all FortiProxy units in the cluster to have the same x-cache-message.
553285	The GUI should allow multiple ports to be added to an Explicit Proxy entry.
553431	When a forwarding server is used in a policy, HTTPS traffic will always fail.
553546	In *FortiView* > *Applications*, the Application column is blank, and the Risk column displays “Unknown.”
553994	When traffic is redirected from a web-proxy policy that matches a session-based user, the authentication and authorization at the SSH-policy level are skipped.
554270	Using HTTPS cert-inspection web filter detection but no server name indication causes a WAD crash.

Bug ID	Description
554271	If deep scan is enabled, FortiProxy should detect the TLS fingerprint using the User-Agent.
554664	The *FortiView* > *Web Sites* page is always blank.
554679	The *FortiView* > *Threats* page is always blank.
554681	After importing a CA certificate on FortiProxy, the CA cache is not updated.
554697	Changing the existing ssl-ssh-profile setting does not update the firewall policy.
554874	Using the VPN Creation Wizard for IPSEC remote access causes an “Unable to setup VPN” error.
555061	When using the SSH tunnel policy, the user ID is not being retrieved.
555264	Using the SSH filter in an SSH-tunnel policy fails to block SSH traffic using an SSH tunnel.
555421	After upgrading to FortiProxy 1.1.2, the WAD process crashes with Signal 6.
555430	When there is an empty BOTNETSET during iptables configuration, FortiProxy fails to match policies.
555532	Session license handling needs to be improved.
556734	The memory usage chart on the GUI dashboard is incorrect.
556741	The VMware OVF file should have 2G memory by default.
556771	The Proxy Session data is incorrectly displayed on the GUI in the Licenses widget and the Proxy Sessions widget.
556792	The DNS filter should be able to be configured for the transparent policy as an UTM feature.
556812	Selecting *OK* in the Policy * Object > Explicit Proxy page does not create or update the explicit proxy entry.
557054	Replacement messages do not have background images.
557071	HTTPS pages cannot be accessed using the explicit proxy.
557103	Some of the fields on the Policy page should be removed.
557229	DNS protection should still work even when a security profile has not been applied to the policy.
557236	DNS traffic on port 53 should be listed in the logs with the correct policy ID number.
557402	WAD crashes when an HTTPS request applies a policy with groups or users.
557457	When an HTTPS request applies a policy with groups, it does not enforce authentication.

Bug ID	Description
557681	Logging in to the FTP server using the explicit FTP proxy fails.
557722	The WAN optimization fields should be hidden from the New Policy page and Edit Policy page when the policy action is “isolate” or “redirect.”
558258	The GUI needs to support backing up and restoring the TLS fingerprint file

Known issues

FortiProxy 1.1.3 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.