FortiProxy Release Notes

Version 2.0.3

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

March 22, 2021

FortiProxy 2.0.3 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
March 22, 2021	Initial release for FortiProxy 2.0.3

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.

Xen Project support

The FortiProxy VM is now supported on the Xen Project hypervisor 7.x.

Loopback interface

You can now configure a loopback interface, which allows users on all physical interfaces to access a captive portal. For example:

```
config system interface
   edit "loopback"
      set ip 10.0.0.2 255.255.255.255
      set allowaccess ping https ssh snmp http telnet radius-acct ftm
      set type loopback
      set snmp-index 4
   next
end
```

Dynamic bypass

You can now use dynamic bypass to create a dynamic list of IP addresses to bypass based on specific HTTP response codes and errors.

You can specify how long an entry stays on the dynamic bypass list from its last hit (`timeout`), the maximum number of dynamic entries (`total-max`), and the maximum number of entries for each server (`server-max`). Use one or more of the following values to create the dynamic bypass list:

Error	Description
connect-error	Connection error.
receive-error	The HTTP response is not received.
non-http	The HTTP protocol is not detected.
400	The HTTP response code is 400.
401	The HTTP response code is 401.
403	The HTTP response code is 403.
405	The HTTP response code is 405.
406	The HTTP response code is 406.

Error	Description
500	The HTTP response code is 500.
502	The HTTP response code is 502.
503	The HTTP response code is 503.
504	The HTTP response code is 504.

To use dynamic bypass:

1. Enable the dynamic-bypass feature and then configure it:

```
config web-proxy dynamic-bypass
   set status enable
   set errors <one_or_more_values_separated_with_a_space>
   set total-max <10-50000 entries>
   set server-max <1-255 entries>
   set timeout <1-21600 minutes>
end
```

2. Enable the dynamic-bypass feature for all HTTP traffic in a transparent policy:

```
config firewall policy
   edit <policy_ID>
      set type transparent
      set dynamic-bypass enable
   next
end
```

3. Optional. View a summary of the dynamic-bypass entries and statistics:

```
diagnose wad dynamic-bypass show
```

4. Optional. Delete the dynamic-bypass entries and statistics:

```
diagnose wad dynamic-bypass flush
diagnose wad dynamic-bypass clear
```

Static virtual IPs

Static virtual IPs are now supported.

Mapping a specific IP address to another specific IP address is usually called Destination NAT (DNAT). When this central NAT table is not used, FortiProxy calls this a virtual IP address (VIP). VIP maps an external IP address to an IP address or address range. The mapping can include all TCP/UDP ports or, if port forwarding is enabled, only specific configured ports. VIPs are typically used to translate external or public IP addresses to internal or private IP addresses. VIPs can be used for reverse proxy to support TCP tunnels for any TCP service.

After you create a VIP, assign it to a VIP group.

To create a virtual IP using the CLI:

```
config firewall vip
```

```
   edit <virtual_IP_name>
      set id <0-65535>
      set comment <string>
      set extip <IP_address or range_of_IP_addresses>
      set mappedip <IP_addresses or range_of_IP_addresses>
      set extintf {any | <interface_name>}
      set arp-reply {enable | disable}
      set portforward {enable | disable}
      set protocol {tcp | udp | sctp | icmp}
      set extport <external_port_or_port_range>
      set mappedport <mapped_port_or_port_range>
      set color <0-32>
   next
end
```

For example:

```
config firewall vip
   edit "viptest"
      set id 0
      set comment ''
      set extip 172.16.80.153-172.16.80.154
      set mappedip "192.168.200.59-192.168.200.59"
      set extintf "port2"
      set arp-reply enable
      set portforward enable
      set color 0
      set protocol tcp
      set extport 8765
      set mappedport 80
   next
end
```

To create an IPv4 virtual IP group using the CLI:

```
config firewall vipgrp
   edit <VIP_group_name>
      set interface {interface_name | any}
      set color <0-32>
      set comments <string>
      set member <VIP_name>
   next
end
```

For example:

```
config firewall vipgrp
   edit "viptestgrp"
      set interface "port2"
      set member "viptest" "viptest2"
   next
end
```

Supported models

The following models are supported on FortiProxy 2.0.3, build 0032:

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 2.0.3:

- 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

Software upgrade path

FortiProxy supports upgrading directly from 1.0.x, 1.1.x, or 1.2.x to 2.0.3.

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 2.0.3 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 2.0.3 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 2.0.3 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 issue has been fixed in FortiProxy 2.0.3. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
606447	Cache collaboration for a round-robin load-balanced HA cluster in Config-Sync mode does not happen until after multiple requests.
654455	Specifying no address in a proxy policy causes all traffic to be allowed.
681854	The user can access the FortiProxy GUI using HTTPS, even though the HTTPS allowaccess setting is not enabled for that port.
684637	The `execute ha manage <ID>` command is not working.
687697	The WAN-optimization daemon (WAD) process crashed with a signal 11 (segmentation fault) when FortiProxy matched an authentication rule with a category proxy address.
687997	When an oversized file is passed through, the log message lacks details.
689591, 689888	The FortiProxy unit does not send the RADIUS accounting packet to the accounting server.
690228	The traffic counter ignores transparent-proxy traffic.
691752	The ICAP server does not respond to an ICAP request from Squid.
691914	SAML-SP needs to be able to work with explicit proxy without the user having to configure no proxy for the captive portal's FQDN.
692980	The secondary VM in an HA cluster shuts down unexpectedly when the number of disks differs between the cluster members.
693286	A programming tool discovered memory corruption.
694585	When proxy-addr or wildcard-fqdn is configured in a transparent proxy policy, the source IP address of HTTP traffic that matches the policy is translated to the outgoing IP address, even though central SNAP map table is empty.
694913	After the FortiProxy unit has been restarted, iptables is empty when the central SNAT has the bypass action configured.
695009	Reliable syslog is not working.
696567	The PAC policy is not synchronized between members of an active-active HA cluster.
697000	The WAD process on the ICAP server crashes when traffic is sent using the explicit proxy policy.

Bug ID	Description
697836	Transferring data using the explicit proxy should be faster.
699220	FortiProxy should allow users to configure high availability (HA) and software-defined network (SDN) connectors before they load a VM license.
700072	The WAD process has a high memory usage on the FortiProxy 400E.
701076	SAML-SP authentication results in multiple WAD crashes.
701177	When the ICAP server is trying to connect, it returns an HTTP code 403 error.
701493	When creating or editing a policy in the GUI, the *Create New* button does not work for configuring filters for the DLP sensor.
701661	The captive portal is using the default certificate, instead of the configured certificate.
701837	The WAD process for the ICAP server crashes randomly.
701841	When there is more than one data disk, the FortiProxy deployment on Amazon Web Services (AWS) fails.
702124	The FortiProxy GUI is not displaying the configured heartbeat interface.
703140	When SNAT IP pools are configured, the interface uses the interface IP address instead of the IP pools when sending out packets.
703478	The WAD process crashes when FortiProxy is authenticating a user and changing the authentication configuration at the same time.
703727	There are two different pages available for configuring the antivirus profile.
703907	When running build 0028, there is HTTP and HTTPS access only to port1.

Known issues

FortiProxy 2.0.3 includes the known issues listed in this section. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

Bug ID	Description
491027, 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.