FortiProxy Release Notes

Version 2.0.5

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

June 14, 2021

FortiProxy 2.0.5 Release Notes

Revision 1

TABLE OF CONTENTS

Change log

Date	Change Description
June 14, 2021	Initial release for FortiProxy 2.0.5

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.

Matching explicit web proxy profiles with authentication rules

When configuring an authentication rule, you can now specify the explicit web proxy profile to match. Use the following CLI commands:

```
config authentication rule
   edit <authentication_rule_name>
      set web-proxy <explicit_proxy_entity>
   next
end
```

Support for alternate DNS servers

You can now specify an alternate primary DNS server and an alternate secondary DNS server that are used only if the DNS resolution of the primary or secondary DNS server results in a name error. Use the following CLI commands:

```
config system dns
   set server-select-method {least-rtt | failover} (The default is least-rtt.)
   set alt-primary <IPv4_address>
   set alt-secondary <IPv4_address>
end
```

Managing the relay-state parameter

You can now control whether the relay-state parameter is limited when it exceeds 80 bytes. By default, this relay-state parameter is not limited. Use the following CLI commands:

```
config user saml
   edit <SAML_server_entry_name>
      set limit-relaystate {enable | disable}
   next
end
```

Caching blocked images

You can now cache blocked images on a local RAM disk so that an administrator can review them.

To manage the blocked-image cache using the CLI:

1. Specify the maximum size of the blocked-image cache and set the caching mode:

   ```
   config system global
      set max-img-cache-size <30-300 MB > (The default is 60 MB.)
      set img-cache-mode {stop | rolling } (The default is rolling.)
   end
   ```

2. Enable the blocked-image cache in the Content Analysis profile:

   ```
   config image-analyzer profile
      edit Content_Analysis_profile_name
         set blocked-img-cache {enable | disable} (The default is disable.)
   ```

```
end
```

3. Optional. Check how full the blocked-image cache is:

```
diagnose wad worker imagecache stats
```

4. Optional. Use one of the following commands to erase all cached blocked images:
   - `diagnose test application wad 101`
   - `diagnose wad worker imagecache flush`

To manage the blocked-image cache in the GUI:

1. Specify the maximum size of the blocked-image cache and set the caching mode:
   a. Go to *System* > *Setting*s.
   b. In the *Maximum Cache Size* field, set how many megabytes the cache can store.
   c. Select *Stop* or *Rolling* for the cache mode.
   d. Click *Apply*.
2. Enable the blocked-image cache in the Content Analysis profile:
   a. Go to *Content Analyses* > *Image Analyses*.
   b. Create or edit a Content Analysis profile.
   c. Enable *Saving Blocked Images*.
   d. Click *OK*.
3. Review the blocked image:
   a. Go to *Log & Report* > *Content Analyses*.
   b. Open an entry for a blocked image.
   c. Click *Show the Image*.

NetHSM integration

You can now integrate a FortiProxy unit with the NetHSM hardware security module (HSM) to retrieve a per-connection SSL session key instead of loading the private key and certificate stored on the FortiProxy unit.

Step 1: Verify the server certificate and the client certificate to establish the SSL connection between the HSM server and the FortiProxy unit, which is the HSM client.

1. Check if the client configured in the HSM server is registered already. If the client has been registered, delete the client before registering it.
2. Get the HSM server's certificate and copy it to a local PC.

Step 2: Generate the intermediate certificate authority (CA) on the FortiProxy unit and store the key pair on the HSM server.

1. Generate the client certificate on the FortiProxy unit.
2. Configure the FortiProxy unit to use the client certificate. Use the following commands:

```
config system nethsm
   set status {enable | disable}
   set vendor SafeNet
   set interface <interface_name>
   set receivetimeout <0-4294967295 ms>
   set ha {enable | disable}
   set ha-status-pulling-interval <0-60 minutes>
```

```
    set rsa-mech-remap {enable | disable}
    config servers
      edit <NetHSM_server_name>
        set server <NETHSM_server_domain_name_or_IP_address>
        set server-cert "<PEM_format_certificate>"
        set htl {enable | disable}
      next
    end
    config slots
      edit <NetHSM_slot_name>
        set id <0-4294967295>
        set password <password>
      next
    end
    config hagroups
      edit <NetHSM_HA_group_name>
        set member <HA_group_members>
      next
    end
  end
```

For example:

```
config system nethsm
  set status enable
  set interface "port1"
  config servers
    edit "us_hsm"
      set server "172.30.30.13"
      set server-cert "-----BEGIN CERTIFICATE-----
      MIIDNzCCAh+gAwIBAgIBADANBgkqhkiG9w0BAQsFADBfMQswCQYDVQQGEwJDQTEQ
      ...
      -----END CERTIFICATE-----"
      set htl disable
    next
  end
  config slots
    edit "fortiproxy"
      set id 0
      set password ENC ...
    next
  end
end
```

3. Display the client certificate:

```
execute nethsm client-cert-show
```

4. If the client certificate is not correct, regenerate it:

```
execute nethsm client-cert-create <country_name_or_county_code> <state>
    <city> <organization> <business_unit> <email_address>
```

5. Export the client certificate to your local PC:

```
execute nethsm client-cert-export tftp <IP_address>
```

6. Copy the client certificate to the HSM server.
7. Use SSH to register the client on the HSM server.

8. Verify that the client was registered successfully on the FortiProxy unit. The slot identifier in the output must be the same as the slot identifier configured under the `config system nethsm` command.

```
execute nethsm diagnose
```

9. Generate the intermediate signing CA on the FortiProxy unit:

```
execute certificate local generate hsm <NetHSM_slot_name> <local_
    certificate_name> <key_size> <host_IP_address_domain_name_email_
    address> <country_name> <state> <city> <organization> <business_
    unit> <email_address>
```

Step 3: Sign the intermediate CA, use it in the SSL deep-inspection profile, and apply the policy to deep-inspection SSL traffic.

1. Sign the certificate signing request (CSR).

```
config certificate local
   edit <local_certificate_name>
      unset certificate
      set csr "-----BEGIN CERTIFICATE REQUEST-----
      …-----END CERTIFICATE REQUEST-----"
   next
end
```

2. Set the certificate again.
3. Configure the SSL deep-inspection profile. For example:

```
config firewall ssl-ssh-profile
   edit "<SSL_deep-inspection_profile_name>"
      config https
         set ports <port_number>
      end
   …
   set caname "<CA_certificate>"
   next
end
```

4. Apply the SSL deep-inspection profile to the firewall policy. For example:

```
config firewall policy
   edit <policy_identifier>
      set type explicit-web
      set explicit-web-proxy "<existing_explicit_web_proxy_profile>"
      ….
      set utm-status enable
      set ssl-ssh-profile "<SSL_deep-inspection_profile_name>"
      set av-profile "<existing_antivirus_profile_name>"
   next
end
```

Step 4: Troubleshooting

- Use a packet capture to check the traffic when the re-signing happened. For example:

```
diagnose sniffer packet "any" 'tcp and port 1792'
```

- Check the traffic log to see if the re-signing failed because of a network failure.

- If there are any changes to the server or client, you need to delete the intermediate CA, delete the server and slot, and then reset the configuration using the following commands:

```
execute nethsm reset
```

- Refer to the HSM product documentation: https://thalesdocs.com/gphsm/luna/7.4/docs/network/Content/Home_network.htm

Supported models

The following models are supported on FortiProxy 2.0.5, build 0049:

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 2.0.5:

- 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 2.0.5.

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 2.0.5 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 2.0.5 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 2.0.5 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 2.0.5. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
701275	There should be DNS logs for explicit proxy when the DNS filter has been applied.
705036	The FortiProxy unit received the ARP replies on the incorrect interfaces.
705707	Enabling the `add-x-cache` CLI setting does not result in the x-cache-message being inserted into the HTTP respond header.
706631	When *DNS Filter* and *DLP* are disabled in *System* > *Feature Visibility* page, the features are still displayed in the GUI.
706633	When *Multiple Security Profiles* is disabled in *System* > *Feature Visibility* page, you can still select more than one security profile in the GUI.
706755	The *Clear Counters* option does not work on the *Policy & Objects* > *Policy* page.
708131	Using wildcards for the proxy address and address group does not work in the source address list in the PAC policy.
708132	Using wildcards for the address group does not work in the address list for Central SNAT.
712387	The Antiphish Block Replacement page has been modified to show the correct reason for blocking.
713483	The epsv command is blocked when the FortiProxy server is using WAN optimization.
713863	When using explicit proxy, the Web Filter profile is not being applied to HTTPS traffic on nonstandard ports.
714617	The WAN-optimization daemon (WAD) crashes after receiving a response from the FTP server when the FTP request was routed directly to the FTP server.
714926	GUI access to the FortiProxy should work when transparent mode is used with the Active-Passive HA configuration.
715231	When an application override is added to the application control profile, it appears at the bottom of the list after the category entries.
715521	Rebooting one of the FortiProxy units in an HA cluster caused the HA cluster members to be unsynchronized.
715691	The *FortiGuard category based filter* and *Static Domain Filter* sections of the *Security Profiles* > *DNS Filter* page are not displayed correctly.

Bug ID	Description
716191	SAML crashes when the group information is not queried.
717007	The setting for the `config system zone` command is not applied when using a transparent firewall policy.
717053	When the ICAP profile is enabled, the GUI displays it as disabled.
717127	When filter overrides are configured for application control in the GUI, they disappear after *Apply* is clicked.
717484	Traffic shaping is not working with explicit proxy.
717527	The wrong web-filter log-type causes the WAD to crash.
718381	Remotely accessing FortiCloud works only when a particular FortiProxy unit is the primary in an HA cluster in Active-Passive mode.
718545	The transparent firewall policy with FSSO authentication only allows HTTP and HTTPS traffic from the FSSO user.
719485	The count of WAD-licensed sessions should not continue to increment after the WAN-optimization connection has ended.
720081	When the WCCP service ID is set to a number higher to or equal to 51, the user should be able to specify the protocol.
720563	When the policy type is set to *SSH Tunnel*, the user should be able to specify the incoming interface.
720711	When the FortiProxy unit is used as the local ICAP server, the FortiProxy unit does not respond to the HTTP request type “PATCH.”
722736	When the policy action is set to redirect, the “Log HTTP Transaction” should be hidden.
723961	The IPS signatures are not added to an IPS sensor on the GUI when the IPS sensor contains a filter.
724282	The local certificate cannot be downloaded from the GUI (*System* > *Certificates*).
724504	A WAD crash occurs sometimes with the explicit policy.
724523	FortiView shows two entries when only one user has been authenticated.
724950	After the number of FortiProxy proxy sessions reaches the maximum, the number of sessions is not reduced after the traffic stops.

Common vulnerabilities and exposures

FortiProxy 2.0.5 is no longer vulnerable to the following CVEs:

- CWE-287

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

Known issues

FortiProxy 2.0.5 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.