# FortiProxy Release Notes

**Version 1.2.2**

**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

January 31, 2020

FortiProxy 1.2.2 Release Notes

Revision 1

# TABLE OF CONTENTS

# Change log

| Date | Change Description |
| --- | --- |
| January 31, 2020 | Initial release for FortiProxy 1.2.2 |

# 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:

- There is now unrestricted memory for all FortiProxy-VM licenses. The licenses still control the maximum number of CPUs and disks.
- You can now monitor the IPsec tunnels in the GUI by going to *FortiView* > *IPsec Monitor*.
- The `config cifs domain-controller` command has changed to `config credential-store domain-controller`.
- A new feature protects against credential phishing. The new antiphishing feature detects and blocks known credentials being sent by web requests. You can enable the new web-antiphishing-log to create a log of any antiphishing matches, except for `exempt`. You can also configure custom pattern-matching rules in the CLI.

**To configure the new antiphishing protection in the web filter:**

```
config webfilter profile
   edit <profile_name>
      set web-antiphishing-log {enable | dis
      config antiphish
         set status {enable | disable}
         set domain-controller <string>
         set default-action {exempt | log | block}
         set check-uri {enable | disable}
         set check-basic-auth {enable | disable}
         set max-body-len <0-4294967295>
         config inspection-entries
            edit "<inspection_target_name>"
               set fortiguard-category
               set action {exempt | block | log}
            next
         end
         config custom-patterns
            edit <target_pattern>
               set category {username | password}
            next
         end
      config web
         set urlfilter-table <ID>
      end
   end
```

| CLI option | Description |
|---|---|
| **config antiphish** | |
| web-antiphishing-log | Enable or disable whether to log any antiphishing matches, except for `exempt`. |
| status | Enable or disable whether the antiphishing feature is used. |
| domain-controller | Enter the name of an existing CIFS domain controller. |

| CLI option | Description |
|---|---|
| default-action | Select the action that occurs when no rule is matched. Select `exempt` to exempt the requests from matching. Select `log` to log all matched requests. Select `block` to block all matched requests. |
| check-uri | Enable or disable whether GET requests are checked for credentials passed using URI parameters. |
| check-basic-auth | Enable or disable whether GET requests are checked for known credentials in the HTTP Basic Auth field. |
| max-body-len | Enter the maximum size of a POST body to check for credentials. The default value is 65536. |
| **config inspection-entries** | |
| fortiguard-category | Enter the FortiGuard category to match. |
| action | Select the action that occurs when there is an antiphishing match. |
| category | Select whether the pattern matches the user name or password field. |
| **config web** | |
| urlfilter-table | Enter the URL filter table ID. |

**To configure the new antiphishing protection in the URL filter:**

```
config webfilter urlfilter
   edit <ID>
      config entries
         edit <ID>
            set antiphish-action {block | log}
         next
      end
   next
end
```

| CLI option | Description |
|---|---|
| antiphish-action | Select the action that occurs when there is an antiphishing match.Select `log` to log all matched requests. Select `block` to block all matched requests. |

For example:

```
config webfilter urlfilter
   edit 10
      set name "filter10"
      set comment ''
      set one-arm-ips-urlfilter disable
      set ip-addr-block disable
      config entries
         edit 2
            set url "172.18.80.73"
```

```
            set type simple
            set action exempt
            set antiphish-action block
            set status enable
            set exempt av web-content
            set web-proxy-profile ''
            set referrer-host ''
        next
    end
  next
end
```

## Supported models

The following models are supported on FortiProxy 1.2.2, build 0280:

- FortiProxy 400E
- FortiProxy 2000E
- FortiProxy 4000E
- FortiProxy VM—VMware, KVM, and HyperV

# Product integration and support

## Web browser support

The following web browsers are supported by FortiProxy 1.2.2:

- 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<br>• CentOS 6.4 (qemu 0.12.1) and later |
| VMware | • ESX versions 4.0 and 4.1<br>• 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 1.2.9 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 1.2.0 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 1.2.0 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 1.2.2. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

| Bug ID | Description |
|---|---|
| 525328 | The external resource needs to support a missing content length. |
| 527467 | The VPN tunnel is not shown in the GUI. |
| 569804 | The CIFS antivirus proxy mode should report the same malware-blocking results in all modes. |
| 577551 | The virus report should send the MD5, SHA-1, and SHA-256 hash of all detected infected files to FortiGuard. |
| 581405 | The CIFS antivirus proxy mode should not allow malware that was blocked with HTTP and FTP. |
| 582475 | The WAN-optimization daemon (WAD) crashes when it processes smb2/cifs. |
| 587758 | The fabric connector should not validate the invalid CIDR format `x.x.x.x/*`. |
| 588262 | The “IP Address Threat Feed” fabric connector is not working. |
| 595924 | Users cannot monitor multiple interfaces in HA mode. |
| 597605 | The FortiProxy unit responds to SNMP queries with 0 for all interface counters. |
| 598932 | After upgrading to FortiProxy 1.2.0, the LACP interface is always down. |
| 603146 | After the destination address is configured in the explicit policy, WAD crashes the first three times the explicit policy is triggered. |
| 603523 | When the DNS filter is configured in the transparent policy, the DNS-filter icon does not display in the Web UI. |
| 604587 | FortiProxy drops related messages with a session ID and tree ID equal to FFFFFFFFFFFFFFFFh, bypasses asynchronous messages, and crashes when caching fully overlapped file chunks. |
| 604595 | The WAD crashes when the client closes the CIFS connection. |
| 605721 | SSL deep inspection causes a certificate error when load-balancing in a Config-Sync cluster. |
| 606277 | RADIUS NAS-IP should not be synchronized with the Config-Sync cluster. |

# Known issues

FortiProxy 1.2.2 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. |