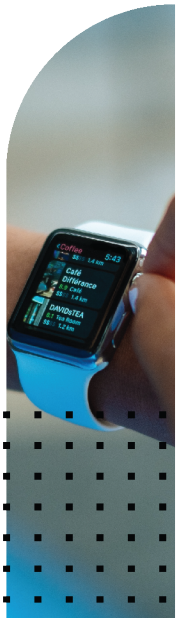
Release Notes

FortiProxy 7.0.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 01, 2023
FortiProxy 7.0.4 Release Notes
45-704-788531-20230601

TABLE OF CONTENTS

Change log

Date	Change Description
2022-04-15	Initial release.
2022-05-25	Added OpenStack version support.
2023-06-01	Added a new feature in What's new on page 7.

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

Supported models

The following models are supported on FortiProxy 7.0.4, build 0078:

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

What's new

The following sections describe the new features and enhancements.

Disabling the IP-based URL rating

You can now enable or disable IP-based URL rating for the SSL/SSH protocol with the following commands:

```
config firewall ssl-ssh-profile
   edit <profile_name>
      set ssl-exemption-ip-rating {enable| disable}
   next
end
```

By default, the IP-based URL rating for the SSL/SSH protocol is enabled.

You can now enable or disable the IP-based URL rating for proxy addresses with the following commands:

```
config firewall profile-protocol-options
   edit <name>
      config http
         set address-ip-rating enable/disable [default:enable]
      end
   next
end
```

By default, the IP-based URL rating for proxy addresses is enabled.

Enabling or disabling reverse DNS lookup

You can now control whether a reverse DNS lookup is performed for policy matching. By default, using reverse DNS lookup is enabled. Use the following commands to change this option:

```
config firewall profile-protocol-options
   edit <name_of_profile>
      config http
         set verify-dns-for-policy-matching {enable | disable}
      end
   next
end
```

New default value for `tcp-window-type` under `config firewall profile-protocol-options`

Under config firewall profile-protocol-options, when configuring HTTP, FTP, SSH, and CIFS, the `set tcp-window-type` option has the following changes:

- New value option `auto-tuning`, which allows the system to automatically tune the TCP window size. When memory usage reaches the threshold of 80%, FortiProxy automatically changes the value to `system` to protect memory usage.
- Default value is changed from `system` to `auto-tuning`.

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.0.4:

- Microsoft Edge 89
- Mozilla Firefox version 87
- Google Chrome version 89

Other web browsers might function correctly but are not supported by Fortinet.

Fortinet product support

- FortiOS 6.x and 7.0 to support the WCCP content server
- FortiOS 6.0 and 7.0 to support the web cache collaboration storage cluster
- FortiManager 7.0.3
- FortiAnalyzer 7.0.2
- FortiSandbox and FortiCloud FortiSandbox, 3.2.1 and 4.0
- FortiAI-VM-KVM 1.5.2

Fortinet Single Sign-On (FSSO) support

- 5.0 build 0301 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 at least 4 GB of 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
OpenStack	• Ussuri

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 7.0.4 or later is 4 GB. You must have at least 4 GB of memory to allocate to the FortiProxy VM from the VM host.

A new FortiProxy VM license file was introduced in the FortiProxy 2.0.6 release. This license file cannot be used for FortiProxy 2.0.5 or earlier. Do not downgrade the FortiProxy 2.0.6 VM because the new VM license cannot be used by earlier versions of the FortiProxy VM.

Upgrading the FortiProxy VM

You can upgrade to FortiProxy 2.0.5 from earlier FortiProxy releases or you can upgrade from FortiProxy 2.0.6 to a higher version. You cannot upgrade from FortiProxy 2.0.5 because of the new FortiProxy VM license file that was introduced in the FortiProxy 2.0.6 release.

If you are upgrading your FortiProxy VM to 2.0.5 or from 2.0.6 and higher, 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 4 GB 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 7.0.4 or later to FortiProxy 2.0.5 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 2 GB 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.

Software upgrade path for physical appliances

When you upgrade from 2.0.x to 7.0.x, you need to click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

You can upgrade FortiProxy appliances directly from 2.0.x to 7.0.4.

If you are upgrading a FortiProxy appliance, use the following procedure:

1. Back up the configuration from the GUI or CLI.
2. Go to *System* > *Firmware* and select *Browse*.
3. Select the file on your PC and select *Open*.
4. Select *Backup Config and Upgrade*.
   Your system will reboot.

Resolved issues

The following issues have been fixed in FortiProxy 7.0.4. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
754289	The WAN-optimization daemon (WAD) crashes with signal 11 when running the autotest group.
764817	You cannot import the Kerberos keytab file unless it has been encoded with base64.
768980	The `set host-regex` command is not working correctly.
770178	When a proxy address is used as the destination in a policy, unrelated traffic matches the policy.
773614	An error message is returned when trying to delete a new admin user in the CLI.
777370	When fast-match is disabled, the HTTPS request fails to match the source proxy address in the policy.
777718	The WAD should use the port in the TCP header to match the service field.
778766	The web proxy does not forward the HTTP request to the forwarding server when FQDN is used to configure the web-proxy forward-server.
782085	Session-based authentication does not redirect the request to the captive portal.
783072	The WAD does not perform a health check for the web-proxy forwarding server.
783145	The Cyrillic alphabet is not displayed correctly in the logs.
783201	Web caching is using too much memory.
783811	The web proxy does not forward requests to the forwarding server when FQDN is used as the address of the forwarding server for web proxy.
783837	After upgrading FortiProxy from an HA cluster, the primary FortiProxy license status changes to “Warning.”
783946	When the source is a ClearPass dynamic object, the explicit proxy policy does not deny the request.
784337	The Open Virtualization Format (OVF) file contains fortios.vmdk instead of fortiproxy.vmdk.
784797	SSH-over-HTTP traffic is redirected to the SSH policy, even when `ssh-policy-redirect` is disabled
784891	When editing a firewall policy in the GUI, the “Proxy Options,” “Disclaimer Options,” and “Security Profiles” sections are missing when the type is set to ssh, ssh-tunnel, wanopt, or ftp.
784974	Computer names are being used for authenticated users, instead of the user names.
785058	The default setting for `servercert` (under the `config vpn ssl settings` command) is null.
785232	The SSL-VPN daemon crashes during a quick HTTP connection from the VPN portal.
785247	When explicit FTP is being used, unknown commands should return a 530 message.
785342	When a proxy request is send using the SOCKS4A protocol, the request fails.

Bug ID	Description
785743	Web application firewall (WAF) profiles block access to hosted websites, instead of illegal HTTP versions.
786194	The *Category Usage Quota* area is missing from the FortiProxy GUI.
787027	The *Content Disarm* options of the antivirus profile are not displayed correctly in the GUI.
787496	There is a WAD memory leak.
788697	After upgrading to FortiProxy 2.0.8, when the type of destination address is set to *URL category*, the URL is blocked. **Workaround:** Use an allow policy in front of the blocking policy.
788698	After upgrading to 7.0.3, the logout page cannot be accessed after logging in with form-based authentication.
789150	The *Duration* field of the HTTP Transaction log shows seconds, instead of milliseconds.
789520	When a policy has the action set to `isolate` and the service set to `http-connect`, websites are not being properly isolated.
789600	When a firewall policy has the proxy-address type set to *URL Category*, the policy does not correctly block the specified categories.
789960	The user cannot create a three-node Config-Sync cluster.
789982	If the URL category is used in the firewall policy, websites are not being properly blocked.
791235	Exempting traffic from SSL inspection in the SSL/SSH inspection profile does not work.
791668	The shaping profile is not being used by the shaping policy.
792579	Implicit Deny Policy logs and HTTP transaction logs are not working.
793251	IPv6 address group objects cannot be added to the policies.
793687	The `set ip-src-port-range` command is not working.
794537	The default value for `set tcp-window-type` (under `config firewall profile-protocol-options`) should be `auto-tuning`.
794753	After upgrading from 7.0.1 to 7.0.3, a proxy user who was authenticated by LDAP cannot access the basic authentication web page.
795159	Traffic is triggering the wrong policy when the source is a proxy-address type header.
795621	When the antivirus profile is using deep inspection, some website uploads are denied.
795970	When the ICAP profile is configured, web pages cannot be fully displayed.
796152	When the transparent proxy is received, there is a WAD memory leak.
796489	The Digest Algorithm options are missing in the FortiProxy GUI.
796574	The authentication scheme for the SAML method cannot be saved in the GUI.

Bug ID	Description
796664	Domain-fronting should be disabled on HTTP2 traffic.
797609	When the IPv6 default route is configured, the gateway route is not installed.
798027	Multiple WAD worker crashes cause the “Access Denied - The Maximum web proxy user limit has been reached.” error to be reported.
798054	When using deep SSL inspection, a web page produces an error but loads eventually.
798745	The original HTTP request should be forwarded to the web server.
799171	The WAD crashes when the configuration is being changed in a transparent firewall policy.
799214	The HTTPS request is not being forwarded to the forwarding server.
799278	The `set dedicated-to management` command (under `config system interface`) is not working correctly.
799847	Sometimes the Internet cannot be accessed when transparent mode, the Internet Service Database, and user authentication are being used together.
800243	The management interface should only listen for ports listed in the `set allowaccess` command.

Common vulnerabilities and exposures

FortiProxy 7.0.4 is no longer vulnerable to the following CVEs:

- CWE-79
- CWE-120
- CWE-124
- CWE-269

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

Known issues

FortiProxy 7.0.4 includes the known issues listed in this section. For inquires about a particular issue, please contact Fortinet Customer Service & Support.

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

www.fortinet.com