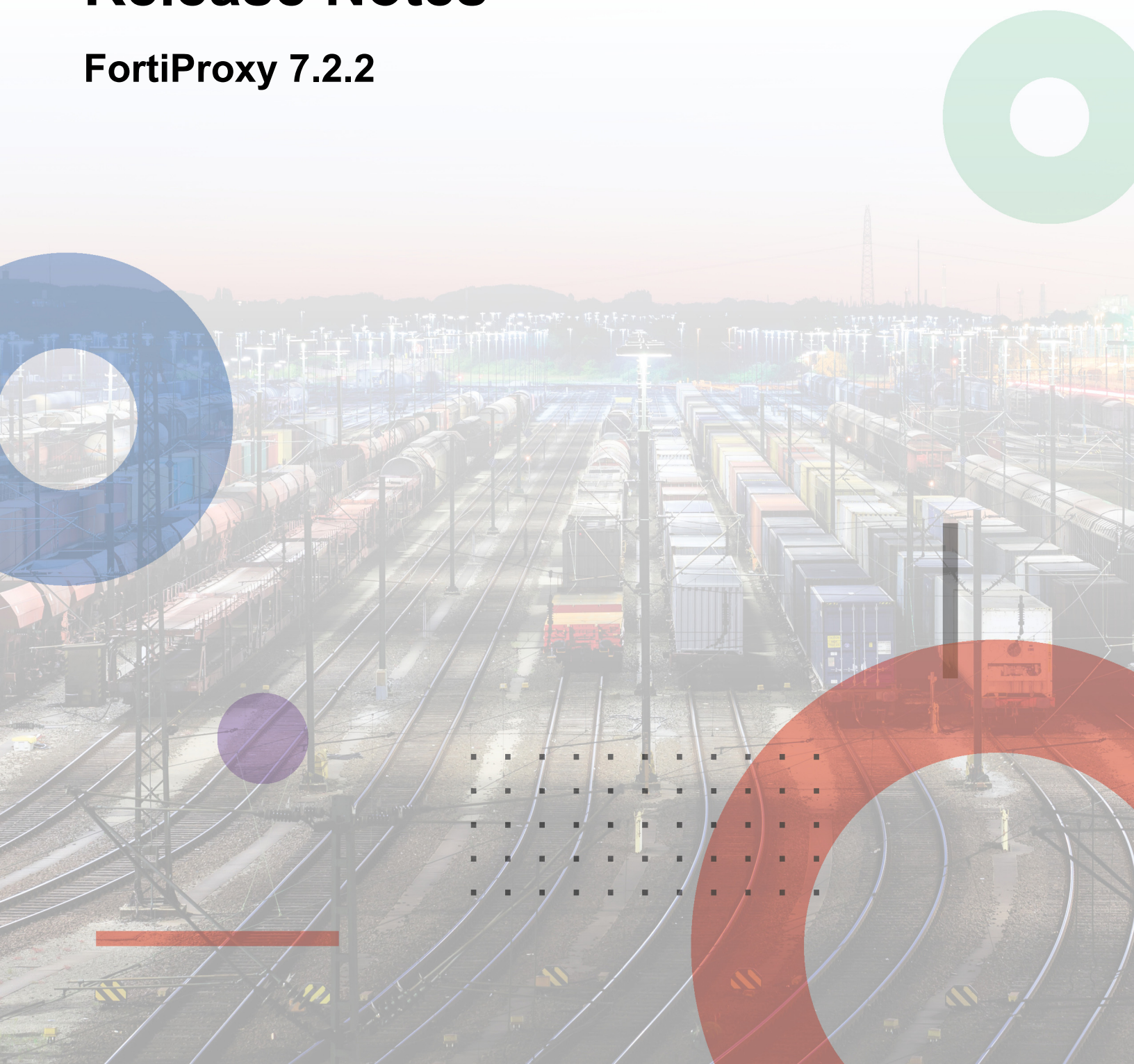
FORTINET

Release Notes

FortiProxy 7.2.2



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

FORTINET VIDEO LIBRARY
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 LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 26, 2023
FortiProxy 7.2.2 Release Notes
45-722-864481-20231026

TABLE OF CONTENTS

Change log

Date	Change Description
2022-12-20	Initial release.
2023-03-07	Added "CVE-2022-45861" to Resolved issues on page 15.
2023-03-09	Added "CVE-2022-42476" to Resolved issues on page 15.
2023-04-11	Added the following CVEs to Resolved issues on page 15: • CVE-2022-41330 • CVE-2022-43947
2023-04-21	Updated Introduction on page 5.
2023-06-13	Added the following CVEs to Resolved issues on page 15: • CVE-2023-26207 • CVE-2022-42474 • CVE-2022-41327
2023-06-23	Updated Product integration and support on page 11.
2023-06-27	Updated Product integration and support on page 11.
2023-10-26	Updated Product integration and support on page 11.

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 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 DLP 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)	IPS 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.
Client-based native browser isolation (NBI)	Client-based native browser isolation (NBI) uses a Windows Subsystem for Linux (WSL) distribution (distro) to isolate the browser from the rest of the computer in a container, which helps decrease the attack surface.

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 7.2.2, build 0333:

FortiProxy	• FPX-2000E • FPX-4000E • FPX-400E
FortiProxy VM	• FPX-AZURE • FPX-HY • FPX-KVM • FPX-KVM-ALI • FPX-KVM-AWS • FPX-KVM-GCP • FPX-KVM-OPC • FPX-VMWARE • FPX-XEN

What's new

The following sections describe new features and enhancements:

Toggle logging pending traffic

Logging pending traffic can be enabled/disabled. When enabled, all traffic, including pending traffic, is logged. When disabled, only traffic matched to a policy is logged. It is disabled by default.

To configure the logging sessions depending on policy matching:

```
config web-proxy global
    set log-policy-pending {enable | disable}
end
```

`enable`	Enable logging sessions that are pending on policy matching.
`disable`	Disable logging sessions that are pending on policy matching (default).

Inter-VDOM links

VDOM links are virtual interfaces that allow VDOMs to communicate internally without using additional physical interfaces. A VDOM link contains a pair of interfaces, each one connected to a VDOM to form each end of the inter-VDOM connection. Inter-VDOM routing can be configured in order to communicate between one VDOM to another.

When VDOMs are configured on your FortiProxy unit, configuring inter-VDOM routing and VDOM links is similar to creating a VLAN interface.

For more information about VDOMs, see Virtual domains.

To create a VDOM link:

1. Enable multi VDOM mode and create the VDOMs.
2. Assign interfaces to VDOMs.

3. Configure the VDOM link:

```
config global
    config system vdom-link
        edit <link name>
        next
    end
end
```

Interfaces of type *vdom-link* are automatically created after configuring a VDOM link. They cannot be directly created. Each link creates two interfaces, named *<link name>0* and *<link name>1*, that can be moved between VDOMs and serve as the inter-VDOM link.

4. Configure inter-VDOM routing:

```
config global
    config system interface
        edit <link name>0
            set vdom <vdom name>
            set ip <ip/netmask>
            set allowaccess https ping ssh
            set description "Far side of the VDOM link"
        next
        edit <link name>1
            set vdom root
            set ip <ip/netmask>
            set allowaccess https ping ssh
            set description "Management side of the VDOM link"
        next
    end
end
```

5. Configure the firewall policies so that the links can be accessed.

Cross-VDOM VLANs

A VLAN can be applied to a VDOM that is different from the VDOM that its physical interface is applied to.

For example:

```
config system interface
    edit port1
        set vdom root
        set ip 10.10.0.254 255.255.255.0
        set allowaccess https ssh
        set type physical
        set snmp-index 1
    next
    edit vlan1
        set vdom Test-VDOM
        set ip 10.123.123.1 255.255.255.0
        set device-identification enable
        set role lan
        set snmp-index 10
        set interface port1
```

```
        set vlanid 1
    next
end</pre>
```

Passive FTP mode for explicit proxy

The FTP mode for explicit proxy can be changed to passive mode. When in passive mode, the FTP client mode is based on the FTP client's preference, while the FTP proxy to FTP server connection is always passive (if supported by the FTP server).

By default, the FTP mode is client, meaning that the FTP mode for both the client and server is based on the FTP client's preference.

To configure the FTP mode for explicit proxy:

```
config ftp-proxy explicit
    set status enable
    set server-data-mode {client | passive}
end
```

client	Use the same transmission mode for client and server data sessions (default).
passive	Use passive mode on server data session.

855703	Add option to use the first hard disk for only logging on high end models.

Use the first hard disk for logging only

On high end models, such as the FortiProxy 2000E and 4000E, the first hard disk can be configured to be used only for logging, as opposed to logging and WAN optimization.

To configure what the first hard disk is used for:

```
config system storage
                        edit "HD1"
                        set usage {mix | log}
                        next
                end
```

mix	Use the hard disk for both logging and WAN Optimization.
log	Use the hard disk for logging.

Toggle TLS fingerprint

The TLS fingerprint can be updated when deep-inspection is enabled. By default, this option is disabled.

```
config system global
    set update-tls-finger-print {enable | disable}
end
```

Support AliCloud platform

FortiProxy-VM supports Alibaba Cloud (AliCloud).

AliCloud Elastic Compute Service (ECS) provides fast memory and the latest Intel CPUs to help you power your cloud applications and achieve faster results with low latency.

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.2.2:

- Microsoft Edge
- 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 - See the FortiManager Release Notes.
- FortiAnalyzer - See the FortiAnalyzer Release Notes.
- FortiSandbox and FortiCloud FortiSandbox- See the FortiSandbox Release Notes and FortiSandbox Cloud Release Notes.
- FortiIsolator 2.2 and later - See the FortiIsolator Release Notes.

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

Fortinet recommends running the FortiProxy VM with at least 4 GB of memory because the AI-based Image Analyzer uses more memory compared to the previous version.

Supported hypervisor versions:

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 6.5, 6.7, and 7.0
Openstack	• Ussuri
Nutanix	• AHV

Supported cloud platforms:

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)
- OCI (Oracle Cloud Infrastructure)
- Alibaba Cloud

Downloading the firmware file

1. Go to https://support.fortinet.com.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support* > *Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiProxy*.
5. On the *Download* tab, navigate to the FortiProxy firmware file for your FortiProxy model or VM platform in the *Image Folders/Files* section. `.out` files are for upgrade or downgrade. `.zip` and `.gz` files are for new deployments.
6. Click *HTTPS* to download the firmware that meets your needs.

Deploying a new FortiProxy appliance

Refer to the FortiProxy QuickStart Guide for detailed instructions of deploying a FortiProxy appliance. Refer to Product integration and support on page 11 for a list of supported FortiProxy units.

Deploying a new FortiProxy VM

Refer to the FortiProxy Public Cloud or FortiProxy Private Cloud deployment guides for more information about how to deploy the FortiProxy VM on different public and private cloud platforms. Refer to Product integration and support on page 11 for a list of supported VM platforms.

Upgrading the FortiProxy

You can upgrade FortiProxy appliances or VMs from 7.0.x or 7.2.x to 7.2.2 by following the steps below:

1. In the GUI, go to *System* > *Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.
5. Click *Continue*.

   The configuration file is automatically saved and the system will reboot.

If you are currently using FortiProxy 2.0.x, Fortinet recommends that you upgrade to 7.0.x first by following the same steps above before attempting to upgrade to 7.2.2.

Upgrading a FortiProxy 2.0.5 VM to 7.0.x requires a different upgrade process with additional backup and configuration as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.

To upgrade a FortiProxy 2.0.5 VM to 7.0.x:

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.

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

Downgrading the FortiProxy

You can downgrade FortiProxy appliances or VMs from 7.2.2 to 7.2.x or 7.0.x by following the steps below:

1. In the GUI, go to *System* > *Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.
5. Click *Continue*.

   The configuration file is automatically saved and the system will reboot.

To downgrade from FortiProxy 7.2.2 to 2.0.x, Fortinet recommends that you downgrade to 7.0.x first by following the same steps above before attempting to downgrade to 2.0.x.

Downgrading a FortiProxy 7.0.x VM to 2.0.5 or earlier requires a different downgrade process with additional backup and configuration as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.

To downgrade a FortiProxy 7.0.x VM to FortiProxy 2.0.5 or earlier:

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.

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

Resolved issues

The following issues have been fixed in FortiProxy 7.2.2. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
550701	Fix signal 6 backtrace is not generated for forticron daemon.
553604	CMDB lock issues.
713286	WAD crash at signal 11 on video filter related process.
742483	Fix random system events log with the message "msg=UrlBwl-black gzopen fail".
764770	Fix external resource download DNS bottleneck.
784326	Flaws in auth_key_encrypt.
784785	Unsupported ZTNA logic prevents proper ZTNA matching. Fix default CA certificate changed to blank after refresh.
789153	A profile with higher privileges than the user's own profile can be set.
793651, 798873, 814265, 831805, 834375, 836260, 842082, 849803, 851521, 856031, 858061, 859390, 859420, 862510, 863235, 863428, 866845, 867418	Fix GUI issues.
807982	Disable group profile with DNS filter in explicit-web policy.
809141	Client hung when FortiAI error encountered with fortiai-error-action as log-only in antivirus profile.
810989	GUI permission override should only apply to GET by default.
814038	Fix VDOM data from leaking to other VDOMs through the REST API (Report Runner and CMDB tables cluster-sync and vdom-property).
818371	Fix WAD process crash at wad_http_req_add_option of wad_http_engine.
818869	FTP traffic does not get redirected to WAD.
819887	GCP does not process multipart MIME data.
823078, 855664, 855853	WAD user-info process randomly consumes 100% CPU of one core.
826254	Fix disk formatting issue after changing usage.

Bug ID	Description
830450	WAD crashes on wad_p2s_ciphers_filter.
832515, 834314	Crash due to connection aborting.
834378	Guest users able to access webpage past the provisioned time allotted for them.
834420, 834729	Extra, unnecessary X-authentication-User/Group field on ICAP header and default ICAP header change
835129	ICAP client header parser cannot handle piggy or sibling flag HTTP headers.
837192	Fix virtual MAC setup in HA mode.
838913	Fix malformed request false positive issue.
839201	ICAP client timeout issue .
840549	Fix WAD unable to recognize RSSO user.
841506	Fix WAD memory spike on ISO file when stream-scan enabled.
841571	Disable VXLAN configuration in transparent mode.
841828	Traffic is not authorized when AD username is provided without a domain.
842764, 845323	Update of VRF with multiple VDOMs.
844990	Enforce IP bans on existing traffic.
845570	Fix for re-compiling `wad_ebpf_dispatcher.c`.
845577	WAD crashes at fts_client_hello_cancel.
845818	Remove the 10 second count down for falling back URL when SSO IdP is not configured.
846630	ZTNA status removed from GUI.
846857	Fix TLS 1.1 certificate-inspection bypass failure.
846870	Allow management access to local interfaces with IPsec and SSLVPN.
847484	Read-only administrators able to sniff other administrators' cookies.
849320	Improve performance when changing the configuration.
849549	In deep-inspection, FortiProxy cannot forward ALPN extension in clienthello to server.
849714	Keep the default value, `disable`, for the `pac-data` field in `config user krb-keytab` when upgrading.
850440	Fix WAD algorithm crash when loading ia-profile.
850558	Webcache is unable to retrieve large cached objects.
850841	Arbitrary read/write vulnerability in custom language.
851134	Change the maximum size allowed for entry names under `config firewall proxy-address` to 80 bytes.

Bug ID	Description
851188	Fix string comparing issue when the host name in the request is capitalized.
851508	FNBI installation failed on version 7.2.1.
851602	FTP over HTTP connect method should not require that ftp-over-http be enabled. Port matching mechanism optimized. Missing semicolon caused a compile error.
852198	Saving issue when adding entries to an Isolator profile.
852416	Trusted host IP table rules are only generated for super administrators.
852416	Non-super administrators are skipped when checking for trusthost wildcards.
852875	WAD memory is not assigned when building JSON responses for isolator.
853406	Fix SSL certificate full check for external resources when the hostname is the IP address.
854176	Patch for arbitrary file deletion in log reports.
854432	Fix TCP port validate return false for proxy SSL redirect.
854469	Fix print mgmt-data syntax errors.
854833	Fix incorrect license information on secondary FortiProxy.
855009	Fix error when adding different URL lists to different URL match ruless.
855603	Fix pipeline requests failure when enabling IPS/APPCTL.
855816	Clone DSCP marker to the other end of transparent proxies.
855838	High latency and CPU usage when deleting webcache entries matching a simple-string URL pattern.
856008	Fix netlink socket not closed when setting up IP pools.
856235	High memory usage by WAD worker in object ssl.fts.str.fstr_buffer_bytes.
857284	Remove NAF.
857338	Fix WAD traffic stats client add stats crash.
857507	WAD crash at `wad_http_fwd_msg_body`.
857530	The image-analyzer profile should be a per VDOM configuration, not a global shared profile,
857691	Remove duplicate `address-ip-rating` in the `profile-protocol-options`.
858488	Fix wa_cs daemon crashes when the request data length is larger than the range data length.
858647	Fix race condition resulting in interfaces being stuck up or down with HA enabled .
858936	Proxy address cannot be selected when editing an isolator profile.
859937	Fix webcache memory leak.
860381	Fix webcache prefetch build crashes when an entry has an empty configuration.
860461	Fix wrong web proxy profile assignment issue.

Bug ID	Description
860495	Decode DLP log URL field to utf-8.
860520	Improve table build speed when policy uses a zone as the soure and/or destination address.
860620	Potential memory leak on DoT traffic.
861151	SSL Mirror does not work.
862001	Prevent password ciphertext exposure in logs.
862130	Fix high data/partition usage.
862846	Configuration Backup and Restore in CLI is not working as expected. The `honor-df`, `send-pmtu-icmp`, and `ipv6-allow-anycast-probe` commands are removed from `config system global`.
864621	SSH public key changes after every reboot
865135	Multipart boundary parsing failed with CRLF before the end of boundary1.
865318	ICAP server with antivirus crash when sending HTTPS to eicar.com .
868043	WAD worker crashes when performing basic local authentication.

Common vulnerabilities and exposures

FortiProxy 7.2.2 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
854181	CVE-2022-42475
854229	CVE-2022-42476
866003	CVE-2022-45861
845849	CVE-2022-41330
862003	CVE-2022-43947
862001	CVE-2023-26207
854176	CVE-2022-42474
847484	CVE-2022-41327

www.fortinet.com