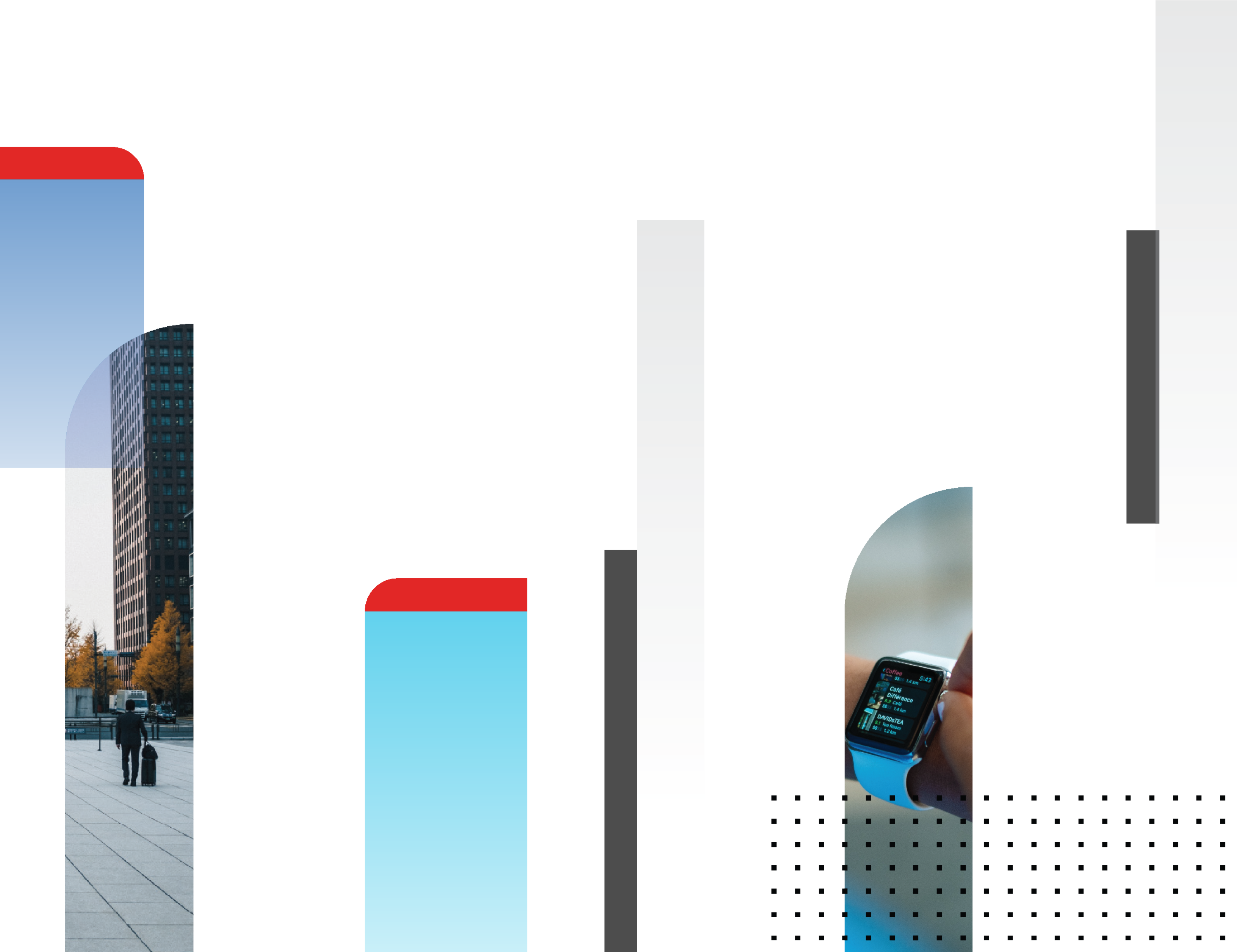
Release Notes

FortiProxy 7.0.6



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

NSE 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

FORTINET®

August 12, 2022
FortiProxy 7.0.6 Release Notes
45-706-831515-20220812

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-08-12	Initial release.

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 7.0.6, build 0102:

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 new features and enhancements:

- Policy based routing on page 7
- Default certificate authority on page 8
- Reauthentication mode configuration on page 8
- Embed images in replacement messages on page 9
- View the IPsec tunnel status in the GUI on page 9
- Webcache prefetch settings on page 10
- ICAP server response extension headers on page 10
- Filter WAD log messages by process types or IDs on page 11

Policy based routing

Policy routing allows you to specify an interface to route traffic. This is useful when you need to route certain types of network traffic differently than you would if you were using the routing table. You can use the incoming traffic's protocol, source or destination address, source interface, or port number to determine where to send the traffic.

To configure a policy-based route in the CLI:

```
config router policy
    edit <name>
        set input-device <interface>
        set src <ip_address/netmask>
        set dst <ip_address/netmask>
        set action {permit | deny}
        set protocol <integer>
        set start-port <port>
        set end-port <port>
        set start-source-port <port>
        set end-source-port <port>
        set gateway <address>
        set output-device <interface>
        set status {enable | disable}
        set comments <string>
    next
end
```

input-device <interface>	Incoming interface name.
src <ip_address/netmask>	Source IP and mask (x.x.x.x/x).
dst <ip_address/netmask>	Destination IP and mask (x.x.x.x/x).
action {permit | deny}	Action of the policy route (default = permit).

protocol <integer>	Protocol number (0 - 255).
start-port <port>	Start destination port number (1 - 65534).
end-port <port>	End destination port number (1 - 65534).
start-source-port <port>	Start source port number (1 - 65534).
end-source-port <port>	End source port number (1 - 65534).
gateway <address>	IP address of the gateway.
output-device <interface>	Outgoing interface name.
status {enable | disable}	Enable/disable this policy route (default = enable).
comments <string>	Optional comments.

Default certificate authority

Default certificate authorities (CA) can be configured and, by default, web-proxy and ssl-ssh-profile use the default CAs:

```
config firewall ssl default-certificate
    set default-ca "Fortinet_CA_SSL"
    set default-untrusted-ca "Fortinet_CA_Untrusted"
    set default-server-cert "Fortinet_Factory"
end
```

```
config web-proxy global
    set ssl-cert "default-server-cert"
    set ssl-ca-cert "default-ca"
end
```

```
confir firewall ssl-ssh-profile
    edit 1
        set caname "default-ca"
        set untrusted-caname "default-untrusted-ca"
    next
end
```

The CA can be changed by either changing the default, or by setting a specific default for the web-proxy or ssl-ssh-profile. For example, to change the web-proxy CAs, but not the defaults:

```
config web-proxy global
    set ssl-cert "Personal_Server_CA"
    set ssl-ca-cert "Personal_CA"
end
```

Reauthentication mode configuration

Configuring the proxy reauthentication mode has changed.

To configure when users must reauthenticate:

```
config system global
    set proxy-keep-alive-mode {session* | traffic | re-authentication}
    set proxy-re-authentication-time <integer>
end
```

`proxy-keep-alive-mode {session* | traffic | re-authentication}`	Control if users must reauthenticate after a session is closed, traffic has been idle, or from the point that the user was first created (default = session): - `session`: Proxy keep-alive timeout begins at the closure of the session (default). - `traffic`: Proxy keep-alive timeout begins after traffic has not been received. - `re-authenticate`: Proxy keep-alive timeout begins when the user was authenticated.
`proxy-re-authentication-time <integer>`	The time limit that users must reauthenticate if `proxy-keep-alive-mode` is `re-authenticate`, in seconds (1 - 86400, default = 30).

The following command is no longer available:

```
config system global
    set proxy-re-authentication-mode {session | traffic | abs-time}
end
```

Embed images in replacement messages

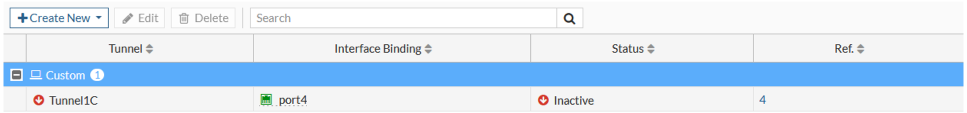
By default, images are embedded in replacement messages instead of using a URL.

To enable/disable embedding images in replacement messages:

```
config webfilter fortiguard
    set embed-image {enable | disable}
end
```

View the IPsec tunnel status in the GUI

Go to *VPN* > *IPsec Tunnels* to view the list of tunnels; the *Status* column shows the status of the tunnel.



	Tunnel	Interface Binding	Status	Ref.
⊟ Custom 1				
	Tunnel1C	port4	Inactive	4

Webcache prefetch settings

To download the prefetch log in the GUI, go to *Web Cache > Prefetch Monitor* and click *Download Prefetch Log*. To configure a prefetch file in the GUI, go to *Web Cache > Prefetch URLs* and click *Create New*. The *Web Cache > Prefetch File* tree menu item is removed.

The `config webcache reverse-cache-prefetch-url` command, and the `prefetch-file` variable under the `config webcache reverse-cache-server` command, are now in the `config webcache prefetch` command:

To configure webcache prefetch in the CLI:

```
config webcache prefetch
    edit <name>
        set url <url>
        set crawl-depth <integer>
        set ignore-robots {enable | disable}
        set interval <integer>
        set start-delay <integer>
        set repeat <integer>
        set user <string>
        set password <password>
        set user-agent {chrome edge firefox safari wget}
    next
end
```

`url <url>`	URL of the target.
`crawl-depth <integer>`	Depth to crawl the whole URL (0 - 16, default = 0).
`ignore-robots {enable | disable}`	Enable/disable ignoring robots.txt file specifications (default = disable).
`interval <integer>`	Time interval to fetch the URL, in seconds (0 - 608400, default = 43200).
`start-delay <integer>`	Delay period to start the fetching, in seconds (0 - 2422800, default = 0).
`repeat <integer>`	How many times repeat to fetch the URL (0 - 4200000000, default = 0).
`user <string>`	Username for the web resource.
`password <password>`	Password for the web resource.
`user-agent {chrome edge firefox safari wget}`	User agents can be used by this prefetch.

ICAP server response extension headers

ICAP server responses can be configured to include X-Virus-ID, X-Infection-Found, and X-Violation-Found extension headers.

```
config icap local-server
    edit 1
        config icap-service
```

```
            edit 1
                set extension-headers {X-Virus-id X-Infection-Found X-Violation-Found}
            next
        end
    next
end
```

`X-Virus-id`	Enable X-Virus-ID ICAP extension header.
`X-Infection-Found`	Enable X-Infection-Found ICAP extension header.
`X-Violation-Found`	Enable X-Violation-Found ICAP extension header.

Filter WAD log messages by process types or IDs

WAD log messages can be filtered by process types or IDs. Multiple process type filters can be configured, but only one process ID filter can be configured.

```
# diagnose wad filter process-type <integer>
# diagnose wad filter process-id <integer>
```

`diagnose wad filter process-type <integer>`	Select process type to filter by (0 - 17, 0 = disable): • 1 = manager • 2 = dispatcher • 3 = worker • 4 = algo • 5 = informer • 6 = user-info • 7 = cache-service-cs • 8 = cache-service-db • 9 = cert-inspection • 10 = YouTube-filter-cache-service • 11 = user-info-history • 12 = debug • 13 = config-notify • 14 = object-cache • 15 = byte-cache • 16 = traffic aggregator • 17 = preload daemon
`diagnose wad filter process-id <integer>`	Select process id to filter by (0 = disable).

To configure multiple filters:

```
# diagnose wad filter process-type 1
# diagnose wad filter process-type 3
# diagnose wad filter process-type 16
# diagnose wad filter process-id 1115
```

To view the configured filters:

```
# diagnose wad filter list
        drop unknown sessions: disabled
        process type:
                manager
                worker
                traffic aggregator
        process id: 1115
```

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.0.6:

- 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.

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.

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.

To upgrade FortiProxy VM to 2.0.5, or from 2.0.6 and later:

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

To downgrade from FortiProxy 7.0.6 or later 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.

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 2.0.6 and later to 7.0.6.

To upgrade a FortiProxy appliance:

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

   The system will reboot.

Resolved issues

The following issues have been fixed in FortiProxy 7.0.6. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
438839, 825139	Replace template image with base64 string instead of URL.
740237, 816913, 818901, 819022, 820242, 821484, 821962, 823091, 824369, 825582, 826385, 827323, 827328	Fix some GUI issues.
741447	Improve keep user login when the original login is still valid after config change.
741736, 741852	Support "FortiView Sessions" page.
742071	In wanopt mode, FortiGate cannot block blocklist certificate.
753479	Fix incorrect history webcache statistics for tp/nontp/tunnel policy.
785584	Fix the issue which "diagnose wad user list" misses policy ID and user group ID.
789960	Fix HA conf-sync issues.
800125	Even if the policy is set to deny FTP_PUT, file uploads are permitted when the UTM feature is enabled.
800129	Change debug log `too-many-users` to `user-restriction` when adding user with existing IP address.
803551	Fix ZTNA VIP address can not be same interface IP address.
804592	Fix LDAP server access under the ha-mgmt interface.
807977, 807995, 808198	FortiNDR log issues of infection cache.
808189	Fix special characters in REST API.
808831	Upgrading to 7.0.5 broke IM controls. Zalo Chat file transfer issues.
810179, 819700	Fix traffic shaping on VLAN interface.
813391	Fix fetching downstream CSF FortiProxy member information.
813562 , 823247, 823829, 829428	WAD user_info process memory leak.
816487	Add a log field called "Prefetch URL" to indicate whether the traffic is from prefetch.

Bug ID	Description
816911	Hide unsupported interfaces for CentralSNAT dstintf.
817699	Upgrade Code for firewall.policy.scan-botnet-connections to ips.sensor.scan-botnet-connects.
818450	Fix dnsproxy config learning issue.
818902	Disabling attributes for HA config-sync.
819204	system.wccp should be hidden when wccp-cache-engine is set as disable.
819236	Static route distance attribute removed.
819764	Fix WAD crashes after soak test.
819850	Fix GUI issues in IPsec Wizard.
819887, 824550	Fixing two cloud-init problems.
820395	FortiProxy returns wrong banner message when operating as FTP proxy.
820636	FortiProxy respondswithe the wrong replacement message when accessing an untrusted site but policy fails to match host part in srcaddr.
820735	Fix the WAD crash when processing the URL filter.
820863	ICAP server config crash issues.
821825	Webcache-https option cannot be enabled when profile-group is configured on firewall policy.
822039	WAD crashed at wad_fmem_free.
822556	Failure to set address group in central-snat rules.
823578, 823962	Fix file-system has smaller size than partition size.
824238	Fix application name field showing "unscanned" in forward traffic log.
824636	Fix mount USB error on system startup.
825384	Fix Traffic volume shows incorrect bandwidth in the user monitor dashboard.
825696	Admin user login should SSH should be denied when a RADIUS Access-Challenge is received with an empty challenge message.
825796	Fix transparent policy mismatch for dst addr when SSL is no_inspection.
826088	Agent-based NTLM authentication resulted in blank user entry and allowed traffic.
826447	FortiGate naming used instead of FortiProxy in readme.txt under the VMware ovf zip file.
826623, 832416, 832469, 832472	GUI improvements: Add domain controller, and Proxy Destination, Sessions, and Source on FortiView.
827037	Add new statistics to report.
827254	Fix server-probe feature.
827710	Fix policy test crash.

Bug ID	Description
828097	Fix Protocol Port Mapping buttons incorrect on SSL-profile.
828766	Port disk number/storage count check from FPX2 to FPX7.
829031	Explicit web with SSL deep inspection and no UTM enabled, HTTPS request failed.
829437	Fix admin WebUI on HTTP and HTTPS not working in L2 TP-mode
829780	Fix static routes in transparent mode cannot set the device to an interface that is dedicated to management. Issue with routes under a dedicated management interface.
831915	Interface option "dedicated-to" hidden on physical FortiProxy models.
832073	WAD crash on wad_http2_session_make().
832582	Fix WCCP Router List IP address tainted when saved by GUI.
832785	Scheduled Prefetch is not removed from the list when the entry is deleted from CLI.
832851	Remove unsupported IPv6 policy route from the GUI.
832863	Fix a kernel panic when running WCCP traffic.
833007	Unable to add IPv6 address to dedicated-to management interface under in transparent mode.
833034	In transparent mode, routes with device set to the management interface should be refreshed when the dedicated-mgmt interface is unset.
833200	Fix probe-response allowance of interface should only allow the corresponding IP address to be accessed on the probe port.
833794	Fix traffic shaping in explicit proxy with HTTPS traffic.

www.fortinet.com