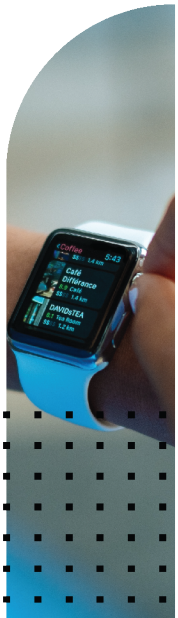
Release Notes

FortiProxy 7.0.2



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

March 22, 2022
FortiProxy 7.0.2 Release Notes
45-702-764854-20220322

TABLE OF CONTENTS

Change log

Date	Change Description
February 7, 2022	Initial release for FortiProxy 7.0.2
February 8, 2022	Updated the “Use DNS over TLS for default FortiGuard DNS servers” and “Add real-time FortiView monitors for proxy traffic” sections.
February 14, 2022	Updated the “Product integration and support” section.
March 22, 2022	Added bug 764817.

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 7.0.2, build 0063:

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:

Zero Trust Network Access (ZTNA)

This section includes information about the following ZTNA new features:

Connect a ZTNA access proxy to an SSL-VPN web portal

SSL-VPN web portals can be defined in ZTNA access proxy settings. The ZTNA access proxy handles the access control processes (client certificate authentication, posture check, user authentication and authorization), and establishes the HTTPS connection between the end user and the access proxy. Then, it forwards the user to the web portal where they can use predefined bookmarks to access TCP based services like HTTPS, RDP, VNC, FTP, SFTP, SSH, Telnet, and SMB. Existing SSL-VPN portal configurations can be used.

The web portal service can only be configured in the CLI.

To configure the SSL-VPN web portal:

1. Go to *VPN* > *SSL-VPN Portals* and click *Create New*.
2. Enter a name, for example, `test_ssl`.
3. Disable *Tunnel Mode*.
4. Enable *Web Mode*.
5. Create the bookmarks:
   a. Under *Predefined Bookmarks*, click *Create New*.
   b. Enter the name of the service.

c. Select the service *Type*.
d. Enter the *URL* to access the service.
e. Click *OK*.
f. Repeat these steps to create other bookmarks.

6. Click *OK*.

To configure the ZTNA access proxy:

1. Configure a VIP for the ZTNA access proxy. The `ssl-certificate` can be replaced with a server certificate:

```
config firewall vip
       edit "ztna_webportal"
               set type access-proxy
               set extip 172.18.62.68
               set extintf "any"
               set server-type https
               set extport 4443
               set ssl-certificate "*.test.com"
       next
end
```

2. Configure the virtual host to be used to connect to the ZTNA access proxy. The host should resolve to the VIP's address:

```
config firewall access-proxy-virtual-host
       edit "webportal"
               set ssl-certificate "*.test.com"
               set host "web.test.com"
       next
end
```

3. Configure the ZTNA access proxy to be in web portal mode:

```
config firewall access-proxy
       edit "ztna_webportal"
               set vip "ztna_webportal"
               set client-cert enable
               config api-gateway
                       edit 1
                               set url-map "/webportal"
                               set service web-portal
                               set virtual-host "webportal"
                               set ssl-vpn-web-portal "test_ssl"
                       next
               end
       next
end
```

4. Apply the access proxy to a proxy policy (specify the ZTNA tags as needed):

```
config firewall policy
       edit 1
               set type access-proxy
               set name "ztna_rule"
               set proxy access-proxy
               set access-proxy "ztna_webportal"
               set srcintf "any"
```

```
                set srcaddr "all"
                set dstaddr "all"
                set ztna-ems-tag "FCTEMS8821000000_High"
                set action accept
                set schedule "always"
                set logtraffic all
                set srcaddr6 "all"
                set dstaddr6 "all"
                set utm-status enable
                set profile-type group
                set profile-group "profile group1"
                set logtraffic-start enable
        next
end
```

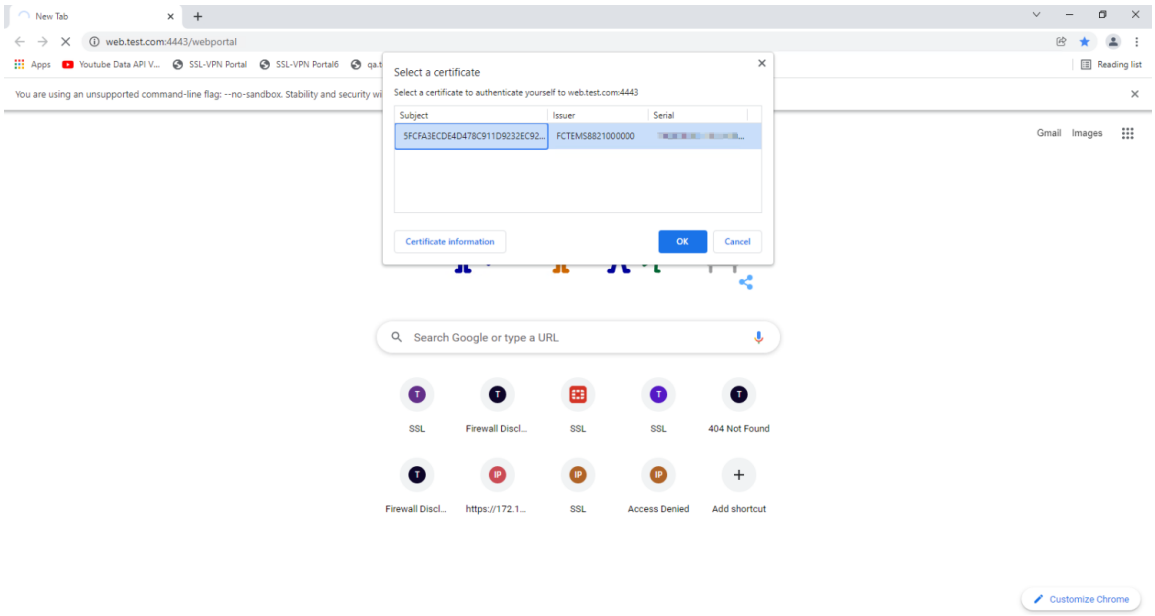
The SSL VPN bookmarks are learned by the WAD daemon and are ready to use.

5. Verify the bookmarks:

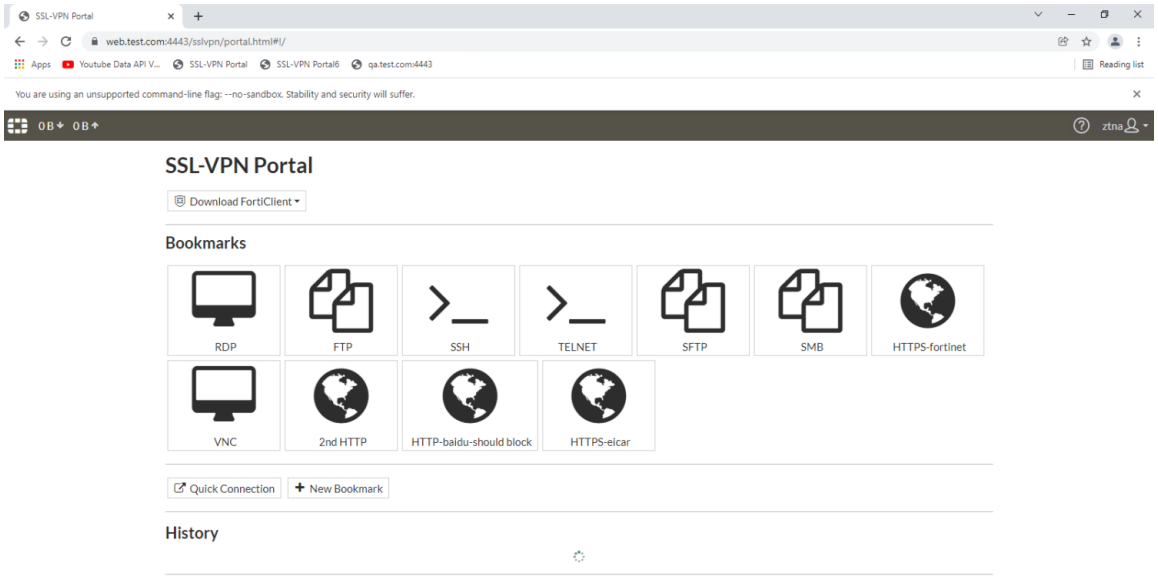
```
# diagnose test app wad 351
[bookmark: (portal/group/name=test_ssl/gui-bookmarks/2nd HTTP)]:
        type  :1
        url   :http://httpbin.org
        host  :
        folder:
        domain:
        port  :0
[bookmark: (portal/group/name=test_ssl/gui-bookmarks/FTP)]:
        type  :4
        url   :
        host  :
        folder:172.16.200.215
        domain:
        port  :0
[bookmark: (portal/group/name=test_ssl/gui-bookmarks/HTTPS-fortinet)]:
        type  :1
        url   :https://www.fortinet.com
        host  :
        folder:
        domain:
        port  :0
[bookmark: (portal/group/name=test_ssl/gui-bookmarks/RDP)]:
        type  :9
        url   :
        host  :172.18.62.213
        folder:
        domain:
        port  :3389
                        …
```

To test the connection:

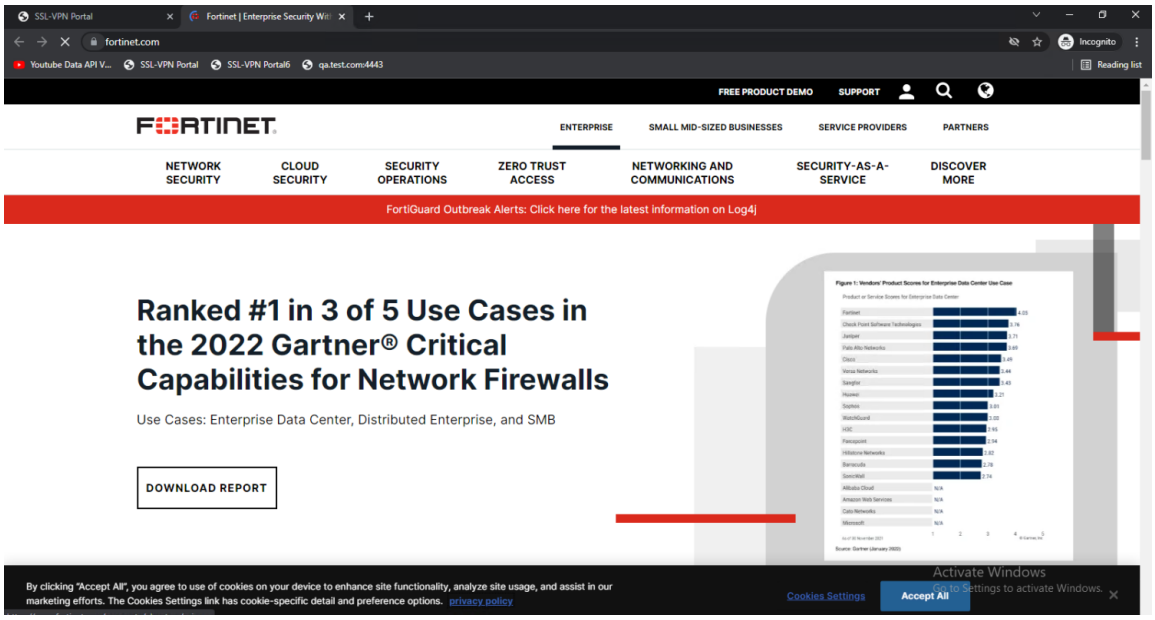
1. From the client browser, go to `https://web.test.com:4443/webportal` to access the ZTNA access proxy web portal.



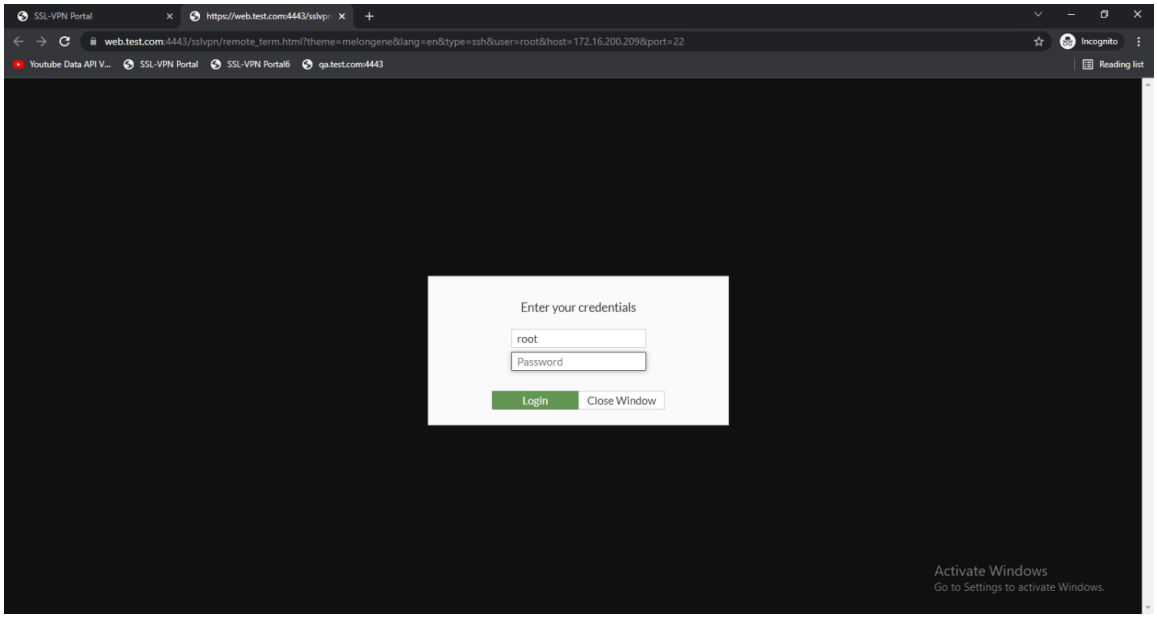
2. Once the client passes the certificate check, posture check, and access is granted, the user is redirected to the web portal. The list of predefined bookmarks appears.



3. Click a bookmark, such as *HTTPS-fortinet*. The website opens.



4. From the web portal, click another bookmark, such as *SSH*. The page opens with the credential login screen to access the server.



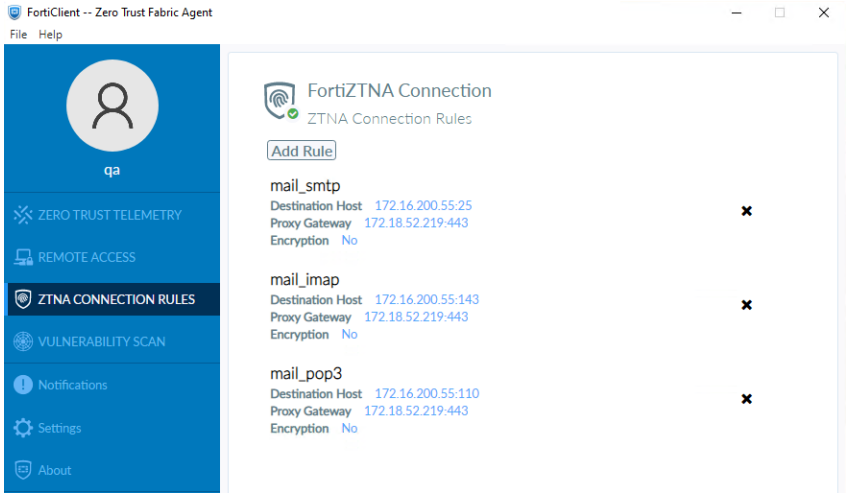
UTM scanning on TCP forwarding access proxy traffic

UTM scanning and deep inspection is supported for multiple protocols in a ZTNA TCP forwarding access proxy. In addition to HTTP and HTTPS, the mail protocols (SMTP, IMAP, and POP3) and file sharing protocols (SMB and CIFS) are supported.

AV scanning for normal POP3, IMAP, and SMTP traffic

To configure AV scanning for normal POP3, IMAP, and SMTP traffic:

1. In FortiClient, add ZTNA connection rules for the email server IP and POP3, IMAP, and SMTP ports.

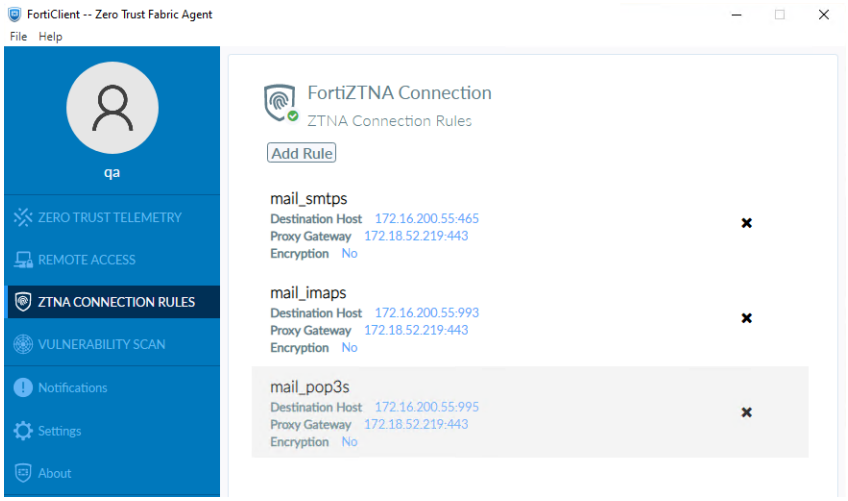


2. In the FortiProxy unit, configure the ZTNA TCP forwarding server to add the email server address and enable AV profile scanning in the ZTNA rules.
3. On the client PC, open Outlook app and send emails with attachments containing virus affected files.
4. The ZTNA rule on the FortiProxy unit blocks the email send/receive traffic and generates AV logs.

AV deep scanning for SSL encrypted POP3S, IMAPS, and SMTPS traffic

To configure AV deep scanning for SSL encrypted POP3S, IMAPS, and SMTPS traffic:

1. In FortiClient, add ZTNA connection rules for the email server IP and POP3S, IMAPS, and SMTPS ports.

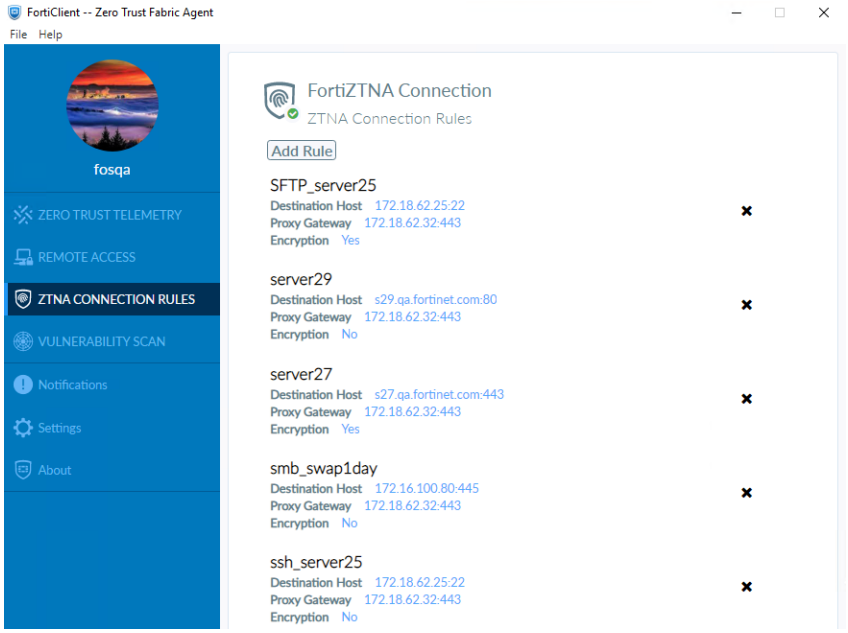


2. In the FortiProxy unit, configure the ZTNA TCP forwarding server to add the email server address and enable AV profile scanning in the ZTNA rules.
3. On the client PC, open Outlook app and send emails with attachments containing virus affected files.
4. The ZTNA rule on the FortiProxy unit blocks the email send/receive traffic and generates AV logs.

AV scanning for SMB service traffic

To configure AV scanning for SMB service traffic:

1. In FortiClient, add ZTNA connection rules for the SMB file sharing server IP and ports.



2. In the FortiProxy unit, configure the ZTNA TCP forwarding server to add the SMB server address and enable AV profile scanning in the ZTNA rules.
3. On the client PC, upload and download virus affected files to and from the SMB server.
4. The ZTNA rule on the FortiProxy unit blocks the email send/receive traffic and generates AV logs.

File filter scanning for CIFS service traffic

To configure file filter scanning for CIFS service traffic:

1. In FortiClient, add ZTNA connection rules for the CIFS server IP and port.
2. In the FortiProxy unit, configure the ZTNA TCP forwarding server to add the CIFA server address and enable file filter profile scanning in the ZTNA rules.
3. On the client PC, upload and download predefined file types (such as .EXE) to and from the CIFS server.
4. The ZTNA rule on the FortiProxy unit blocks the email send/receive traffic and generates AV logs.

Increase ZTNA and EMS tag limits

The following limits have increased for EMS server, IP addresses, and MAC addresses in EMS and ZTNA tags:

- The maximum number of EMS servers a FortiProxy unit can connect to increased from three to five.
- The maximum number of IP address an EMS tag can resolve increased from 1000 to over 100,000.
- The maximum number of MAC address an EMS tag can resolve increased from 1000 to 3000.

Use the following diagnose commands to verify address information:

```
# diagnose firewall fqdn <option>
```

Option	Description
`list-ip`	List IP FQDN information.
`list-mac`	List MAC FQDN information.
`list-all`	List FQDN information.
`getinfo-ip`	Get information of IP FQDN address.
`getinfo-mac`	Get information of MAC FQDN address.
`get-ip`	Get and display one IP FQDN address.
`get-mac`	Get and display one MAC FQDN address.

Use FQDN with ZTNA TCP forwarding access proxy

When defining ZTNA connection rules on FortiClient for TCP forwarding, it is sometimes desirable to configure the destination host address as an FQDN address instead of an IP address. Because the real servers are often servers in the corporate network, this layer of obfuscation prevents internal IP addresses from easily leaking to the public, and also makes the destination more easily recognizable by the end users.

One obstacle to overcome is getting remote hosts to resolve an internal FQDN that is typically only resolvable by an internal DNS in the corporate network. This can be solved with the following:

1. When an FQDN address is added as a destination host in a ZTNA connection rule, FortiClient creates a virtual IP address for this FQDN address and adds this to the computer's host file (Windows). The same is true when a ZTNA connection rule entry is pushed from EMS.
2. The virtual IP address mapped to the FQDN address is not the real address of the server. It allows applications to resolve the FQDN address to this virtual IP address. FortiClient listens to any traffic destined for it and forwards the traffic using the TCP forwarding URL with FQDN to the ZTNA access proxy.
3. The FortiProxy access proxy will resolve the FQDN using the internal DNS on the corporate network, matching the traffic to the ZTNA real server configuration with the same domain and address.
4. If a valid ZTNA real server entry is found, traffic is forwarded to the real server.

This features requires a minimum FortiClient and FortiClient EMS version of 7.0.3.

To configure the TCP forwarding access proxy:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Servers* tab.
2. Click *Create New*.
3. Enter a *Name*, such as `ZTNA_S1`.
4. Configure the network settings:
   a. Set *External interface* to *any*.
   b. Set *External IP* to *172.18.62.32*.
   c. Set *External port* to *443*.
5. Select the *Default certificate*. Clients will be presented with this certificate when they connect to the access proxy VIP.

6. Add server mapping:
   a. In the *Service/server mapping* table, click *Create New*.
   b. For *Service*, select *TCP Forwarding*.
   c. Add a server:
      i. In the *Servers* table, click *Create New*.
      ii. Create a new FQDN address for the HTTPS server at `s27.qa.fortinet.com` and then click *OK*.
      iii. Apply the new address object as the address for the new server.
      iv. Click *OK*.
   d. Add another server using the same steps for `s29.qa.fortinet.com`.
7. Click *OK*. Now that the ZTNA server is complete, the domain settings must be configured in the CLI to map domains to the real servers.

To map domains to the real servers:

```
config firewall access-proxy
       edit "ZTNA_S1"
               set vip "ZTNA_S1"
               set client-cert enable
               config api-gateway
                       edit 2
                               set url-map "/tcp"
                               set service tcp-forwarding
                               config realservers
                                       edit 4
                                               set address "s27.qa.fortinet.com"
                                               set domain "qa.fortinet.com"
                                       next
                                       edit 5
                                               set address "s29.qa.fortinet.com"
                                               set domain "qa.fortinet.com"
                                       next
                               end
                       next
               end
       next
end
```

To configure the ZTNA rule:

1. Go to *Policy & Objects* > *ZTNA* and select the *ZTNA Rules* tab.
2. Click *Create New*.
3. Set *Name* to *ZTNA_TCP*.
4. Set *Incoming Interface* to *port2*.
5. Set *Source* to *all*.
6. Select the ZTNA server *ZTNA_S1*.
7. Configure the remaining options as needed.
8. Click *OK*.

To configure the DNS entries for each server:

1. Enable the DNS database visibility:
   a. Go to *System* > *Feature Visibility*.
   b. Enable *DNS Database*.
   c. Click *Apply*.
2. Go to *Network* > *DNS Service*. Under *DNS Database*, click *Create New*.
3. Set *DNS Zone* to *ZTNA*.
4. Set *Domain Name* to *qa.fortinet.com*.
5. Add the DNS entries:
   a. Under *DNS Entries*, click *Create New*.
   b. Set *Hostname* to *s27*.
   c. Set *IP Address* to the HTTPS server address.
   d. Click *OK*.
   e. Add another DNS entry using the same steps for the s29.qa.fortinet.com HTTP server.
6. Click *OK*.

Testing the connection to the access proxy

Before connecting, users must have a ZTNA connection rule in FortiClient.

ZTNA TCP forwarding rules can be provisioned from the EMS server. See Provisioning ZTNA TCP forwarding rules via EMS for more details.

To create the ZTNA rules in FortiClient and connect:

1. From the *ZTNA Connection Rules* tab, click *Add Rule*.
2. Create a rule for the HTTPS server:
   a. Set *Rule Name* to *server27*.
   b. Set *Destination Host* to *s27.qa.fortinet.com:443*.
   c. Set *Proxy Gateway* to *172.18.62.32:443*.
   d. Disable *Encryption*.
   e. Click *Create*.
3. Create a rule for the HTTP server:
   a. Set *Rule Name* to *server29*.
   b. Set *Destination Host* to *s29.qa.fortinet.com:80*.
   c. Set *Proxy Gateway* to *172.18.62.32:443*.
   d. Disable *Encryption*.
   e. Click *Create*.
4. Upon creating the ZTNA rules, two new entries are added to the Windows PC's host file in folder C:\Windows\System32\drivers\etc. View the file, and observe the new entries for the virtual IP and FQDN pairing for each ZTNA connection rule.

```
# ----- FORTICLIENT ZTNA VIP START -----
10.235.0.1 s27.qa.fortinet.com
10.235.0.2 s29.qa.fortinet.com
# ----- FORTICLIENT ZTNA VIP END -----
```

5. The Windows PC now resolves the FQDNs to the virtual IPs, and FortiClient will listen to the traffic to these IPs and forward them to the TCP access proxy.
6. Have the remote user connect to the HTTPS and HTTP servers on a browser. After device verification, the user is able to successfully connect to the remote servers.

Display EMS ZTNA and endpoint tags in user widgets and Asset Identity Center

EMS ZTNA and endpoint tags are displayed in the *Device Inventory* widget, *FortiClient* widget, and the *Asset Identity Center* page. In the backend, EMS ZTNA tags, endpoint tags, and EMS serial numbers have been added to the user device query API and response.

The ZTNA tag name can be used as a search criterion in the *Asset* view of the *Asset Identity Center* page.

FQDNs supported for ZTNA TCP forwarding

Fully qualified domain names (FQDNs) can now be used for ZTNA TCP forwarding.

SSL VPN

This section includes information about the following SSL-VPN new features:

- WebSocket SSL-VPN tunnel support on page 17
- Azure Active Directory supported for the LDAP authentication source on page 17

WebSocket SSL-VPN tunnel support

The WebSocket SSL-VPN tunnel is now supported for the Chromebook plugin. Only version 13 of the SEC WebSocket protocol is supported.

Azure Active Directory supported for the LDAP authentication source

You can now authenticate user credentials on the FortiProxy unit with Azure Active Directory (AD) services.

REST API

This section includes information about the following REST API new features:

Log REST API events

The REST API events log subtype logs POST, PUT, DELETE, and GET REST API requests. Logs can be viewed under *Log & Report* > *Events* > *REST API Events* after REST API events logging has been enabled in the CLI.

To enable REST API events logging in the CLI:

```
config log setting
       set rest-api-set {enable | disable}
       set rest-api-get {enable | disable}
end
```

`rest-api-set {enable | disable}`	Enable/disable logging of POST, PUT, and DELETE REST API requests.
`rest-api-get {enable | disable}`	Enable/disable logging of GET REST API requests.

Replace FSSO-based FortiNAC tag connector with REST API

A new REST API endpoint in both FortiNAC and FortiProxy is used by FortiNAC to send user logon and logoff information to the FortiProxy unit. The new FortiNAC tag dynamic firewall address type is used to store the device IP, FortiNAC firewall tags, and FortiNAC group information sent from FortiNAC by the REST API when user logon and logoff events are registered.

REST API filter standardization

The following API endpoints now use the same filtering as the `/api/v2/cmdb/` endpoints:

- `/api/v2/monitor/fortiview/statistics`
- `/api/v2/monitor/user/device/query`

Other new features and enhancements

This section includes information about the following new features and enhancements:

Implicit enforcement of deep inspection for user friendly policy matching

When the HTTP CONNECT request or the Transport Layer Security (TLS) server name indication (SNI) partially matches a policy with deep inspection is enabled, deep inspection of the policy is enforced with the HTTPS traffic.

Monitoring the status of the PSUs

A log message is generated if a FortiProxy power supply unit (PSU) loses or regains power.

NOTE: This feature is available only for the FortiProxy 2000E and 4000E models.

Limiting the access of nondomain users

- You can now limit the access of nondomain users while using proxy authentication. To do so:
  - Use the negotiate authentication scheme.
  - Disable NTLM negotiation.

  For example:

```
config authentication scheme
   edit "negotiateonly"
      set method negotiate
      set negotiate-ntlm disable
      set kerberos-keytab "fpx45.dev.fgt.com"
   next
end
config authentication rule
   edit "negotiaterule"
      set srcaddr "all"
      set dstaddr "all"
      set srcaddr6 "all"
      set active-auth-method "negotiateonly"
   next
end
```

Migrating FortiToken Mobile users from the FortiProxy unit to FortiToken Cloud

The `execute fortitoken-cloud migrate-ftm <license> <vdom>` command allows the migration of FortiToken Mobile users from the FortiProxy unit to FortiToken Cloud. The FortiToken Cloud account must be using a time-based subscription license. A request must be made to Fortinet Customer Service to initiate and pre-authorize the transfer. All current active FortiToken Mobile users will be migrated to the FortiToken Cloud license with no changes to the FortiToken Mobile serial number. The FortiProxy user or administrator's two-factor setting is automatically converted from `fortitoken` to `fortitoken-cloud`. After migration, end users will be able to authenticate as before without any changes to their FortiToken mobile app.

Use DNS over TLS for default FortiGuard DNS servers

When using FortiGuard servers for DNS, the FortiProxy unit defaults to using DNS over TLS (DoT) to secure the DNS traffic. New FortiGuard DNS servers are added as primary and secondary servers.

Because DNS servers probably do not support low encryption DES, low encryption devices do not have the option to select DoT or DoH. The devices default to cleartext (UDP/53) instead.

The FortiGuard DNS server certificates are signed with the globalsdns.fortinet.net hostname by a public CA. The FortiProxy unit verifies the server hostname using the `server-hostname` setting.

When upgrading to 7.0.2, the FortiGuard servers are updated to the new defaults.

To view the FortiGuard server DNS settings in the GUI:

1. Go to *Network* > *DNS Settings*.
2. For *DNS servers*, select *Use FortiGuard Servers*. The *Primary DNS server* is *96.45.45.45*, and the *Secondary DNS server* is *96.45.46.46*. *DNS Protocols* is set to *TLS* and cannot be modified.

To view the FortiGuard server DNS settings in the CLI:

```
# show system dns
config system dns
       set primary 96.45.45.45
       set secondary 96.45.46.46
       set protocol dot
       set server-hostname "globalsdns.fortinet.net"
end
```

The `protocol` and `server-hostname` settings should not be modified when using the default FortiGuard servers.

Add real-time FortiView monitors for proxy traffic

The following real-time FortiView monitors have been added for proxy traffic: *FortiView Proxy Destinations*, *FortiView Proxy Sessions*, and *FortiView Proxy Sources*. Proxy policy sessions are no longer shown in the *FortiView Policies* and *FortiView Applications* monitors.

Prerequisites:

1. Configure an explicit proxy and proxy policy.
2. Change the network settings on the client PC to use the FortiProxy unit as the proxy.
3. Generate web traffic on the client PC.

To add the proxy traffic related widgets:

1. Go to *Dashboard* > *Status* and click *Add Widget*.
2. In the *FortiView* section, click the + beside one or all of the following:
   a. *FortiView Proxy Destinations*
   b. *FortiView Proxy Sessions*
   c. *FortiView Proxy Sources*
3. Click *Add Widget*. The widgets are added to the dashboard.
4. Double-click or right-click an entry in a monitor and select *Drill Down to Details* to view additional information about the selected traffic activity.

Process monitor

The *Process Monitor* displays running processes with their CPU and memory usage levels. Administrators can sort, filter, and terminate processes within the *Process Monitor* pane.

To access the process monitor:

1. Go to *Dashboard* > *Status*:
   - Left-click in the *CPU* or *Memory* widget and select *Process Monitor*.
   - Click the user name in the upper right-hand corner of the screen, then go to *System* > *Process Monitor*.

   The *Process Monitor* appears, which includes a line graph, donut chart, and process list.
2. Click the + beside the search bar to view which columns can be filtered.

To kill a process within the process monitor:

1. Select a process.
2. Click the *Kill Process* dropdown.
3. Select one of the following options:
   - *Kill*: the standard kill option that produces one line in the crash log (`diagnose debug crashlog read`).
   - *Force Kill*: the equivalent to `diagnose sys kill 9 <pid>`. This can be viewed in the crash log.
   - *Kill & Trace*: the equivalent to `diagnose sys kill 11 <pid>`. This generates a longer crash log and backtrace. A crash log is displayed afterward.

Add WebSocket for Security Fabric events

With the WebSocket for Security Fabric events, subscribers to the WebSocket (such as the *Fabric Management* page) are updated upon new Fabric events and alert users to reload the page.

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.0.2:

- 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

New deployment of the FortiProxy VM

The minimum memory size for the FortiProxy VM for 7.0.2 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 7.0.2 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

You can upgrade FortiProxy appliances directly from 2.0.x to 7.0.2.

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

Bug ID	Description
681854, 743805, 753747, 758753	Users can still log in to the FortiProxy GUI, even with HTTP and HTTPS access disabled for the interface.
684640	On the FPX-2000E, the HA monitor does not failover when the monitored port is down.
690810	There was a missing break in the WAN optimization explicit proxy component.
741568	After activating FortiCloud, the user could not enable FortiSandbox Cloud.
743029	When upgrading from FortiProxy 2.0 to 7.0, the remote certificates are lost, and the firewall profile protocol options change to the default setting.
743746	The WAD crashes with signal 11 when upgrading to FortiOS 6.2.9 build 9108.
744855	After upgrading from FortiProxy 2.0.5 to 2.0.6, some of the commands under `config firewall profile-group` are missing.
746009	The IP pool configuration in an explicit policy is ignored on outbound traffic.
752944	LACP fails when an HA cluster is configured.
753947	There are too many TIME_WAIT sessions after the admin user logs in to the GUI.
753952	The `set ssl-ssh-profile` command works in the CLI but not in the GUI.
754298	The WAD crashes with signal 11 when running the autotest group.
754575	Users cannot download the PAC file when the pac-file-server-port is set to a different port than the proxy port.
755298	When the policy is in proxy mode and DPI is enabled, the connection to Callone Accession Meeting fails.
755861	When upgrading FortiProxy, the units for the proxy-auth-timeout value need to be converted.
756293	The aggregate interface cannot be used as the HA management interface.
756526	The `diagnose firewall dynamic list` and `diagnose firewall dynamic address` commands are missing for ZTNA tags.
756720	There was a crash on the ICAP server when antivirus scanning and DLP were enabled.
756844	The WAD crashes on the ICAP client with signal 11.
757212	Using transparent mode and the VMware SDN connector results in “response fails schema validation” errors.

Bug ID	Description
757452	Traffic shaping using the Internet Service does not work.
758458	The FortiProxy VM in Azure does not restart properly after the `execute reboot` command.
758947	After creating an HA cluster in Config-Sync mode, the FortiProxy units cannot be accessed because of a memory leak.
759132	After an existing aggregate interface is deleted, the forticron application crashes.
759204	The explicit proxy settings differ in the CLI and GUI.
759216	From the *System* > *Replacement Messages* page, some of the pages mention FortiGate instead of FortiProxy.
759220	Trying to preload cache content results in error 255.
759646	After adding the Quarantine Monitor widget to the dashboard, the new widget does not load data.
759985	When a policy has Internet service addresses in the Destination field, the Destination field is blank in the GUI.
760022	The Safe Search option is available in the CLI but not in the GUI.
760371	You cannot import a certificate without adding a password.
760529	When *Isolate* is selection for the action in a new policy, some options are missing in the GUI.
760550	The DLP log cannot be viewed in the GUI.
760642	The HTTP Proxy-Authorization/Authorization header needs to be removed to prevent user credential leaking.
760817	After FortiProxy is upgraded from 2.0.6 to 7.0.1, the UUIDs do not match in the proxy address groups in an HA cluster.
760835	The WCCP cache engine cannot be enabled or disabled in the GUI.
760840	DNS protection not working in the transparent proxy policy.
761568	The WAD crashes multiple times after the user upgrades from FortiProxy 2.0.6 to 7.0.1.
761732	The `diagnose hardware deviceinfo nic` command does not work in FortiProxy 7.0.1.
762511	The `set http-view` command does not appear under `config system global`.
763023	FortiManager 7.0.3 does not support FortiProxy 7.0.1.
764062	After upgrading from FortiProxy 2.0 to 7.0, the fields of the antivirus profile are unset.
764462	After using the `set ha-mgmt-status disable` command, connecting with Telnet does not work.
764978	Zero-trust network access traffic needs to keep the setting of the source-affinity flag.
764990	Upgrading the firmware of a FortiProxy unit that is a member of an HA Config-Sync cluster causes a wa_cs crash.
765553	After upgrading to build 0051, CRWL keeps crashing.

Bug ID	Description
765806	When the destination is ISDB for a transparent policy, traffic is not forwarded.
768361	When ICAP is enabled for web proxy and cURL is used to send a file, the contents of the *Submitted By* field are corrupted.
768699	The WAD crashes if the authentication rule configuration is updated while WAD is synchronizing.
768980	The `set host-regex` command is not working correctly.
769398	When the ICAP local server is configured, the ICAP server crashes.
769601	When traffic is sent to a transparent proxy policy, the FortiProxy unit crashes.
770178	When a proxy address is used as the destination in a policy, unrelated traffic matches the policy.
770941	URL filter is not blocking a specific page while allowing access to other pages for that domain.
771051	The following commands do not work: • `diagnose ipv6 neighbor-cache list` • `diagnose ipv6 route list` • `diagnose ipv6 address list`
773465	When antivirus caching and inspect-all are enabled, the cached infection scanning results are not used in the FTP download.
773614	After deleting a new system administrator, the CLI responds with an error message, “Add table index error: type=4.”
773909	Preloading cache content fails with error 4 and causes a WAD crash.
774191	The `set ztna-ems-tag` command is not working.
774373	The infection cache needs to skip content when the size is 0.
774567	After upgrading the Azure FortiProxy VM from build 0050 to build 0054, the VM does not start.
774642	After upgrading the GCP FortiProxy VM from build 0047 to build 0054, the VM keeps restarting.
775247	The WAD keeps crashing when the service for the IPv4 API gateway is set to the web portal without a predefined bookmark.
775513	There is a MAC address conflict after enabling the LAG interface in FortiProxy 7.0.1.
775626	Upgrading the firmware in an HA Config-Sync cluster fails.
775648	The forward traffic logs do not display the FSSO user names.
776242	The `config web-proxy explicit` command has been changed to `config web-proxy explicit-proxy`.
776276	After upgrading from FortiProxy 2.0.7 to 7.0.0, multiple errors 160 are logged.
776549, 776550	There was an unintentional integer overflow in the WAN optimization explicit proxy component.
776577	A dereference-after-null-pointer problem was found in the WAN optimization explicit proxy component.

Bug ID	Description
776578	The wrong sizeof argument was used in the WAN optimization explicit proxy component.
776619	After FortiProxy is upgraded to build 0057, the WAD keeps crashing.
776623	The FortiProxy 400E reports that “Maximum WAD worker count 4 is not equal to current cpu number.” when it starts.
776877	When the ICAP server returns an HTTP message other than 200, the client gets an empty reply instead of the actual HTTP message.
776917	The HTTP and HTTPS daemon keeps crashing.
777082	When the FortiProxy unit is in transparent mode, NTLM authentication does not work.
777344	A WAD memory leak occurs when using ICAP.
777364	After the web-proxy entry is deleted, the WAD must be manually restarted for the change to be learned.
777370	When fast-match is disabled, the HTTPS request fails to match the source proxy address in the policy.
777405	After the policy type is changed to explicit, the address in the firewall policy cannot be edited in the GUI.
777544	When using the Active-Passive mode in an HA cluster, the primary unit crashes during synchronization.
777718	The WAD should use the port in the TCP header to match the service field.
778656	When the FortiProxy units are in HA Config-Sync cluster, the secondary unit displays `ha req read header error:1 type:59` in the console.
778659	When proxy inspection is enabled with at least one flow feature (such as IPS or Application Control), all connections to all websites fail and an ERR_EMPTY_RESPONSE is reported.
778992	The load-balancing server list for ICAP cannot be edited in the GUI.

Common vulnerabilities and exposures

FortiProxy 7.0.2 is no longer vulnerable to the following CVEs:

- CWE-79
- CWE-120
- CWE-124
- CWE-134
- CWE-190
- CWE-347
- CWE-550
- CWE-788

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

Known issues

FortiProxy 7.0.2 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.
764817	You cannot import the Kerberos keytab file unless it has been encoded with base64. **Workaround:** Encode the Kerberos keytab file with base64 before importing it into FortiProxy.

www.fortinet.com