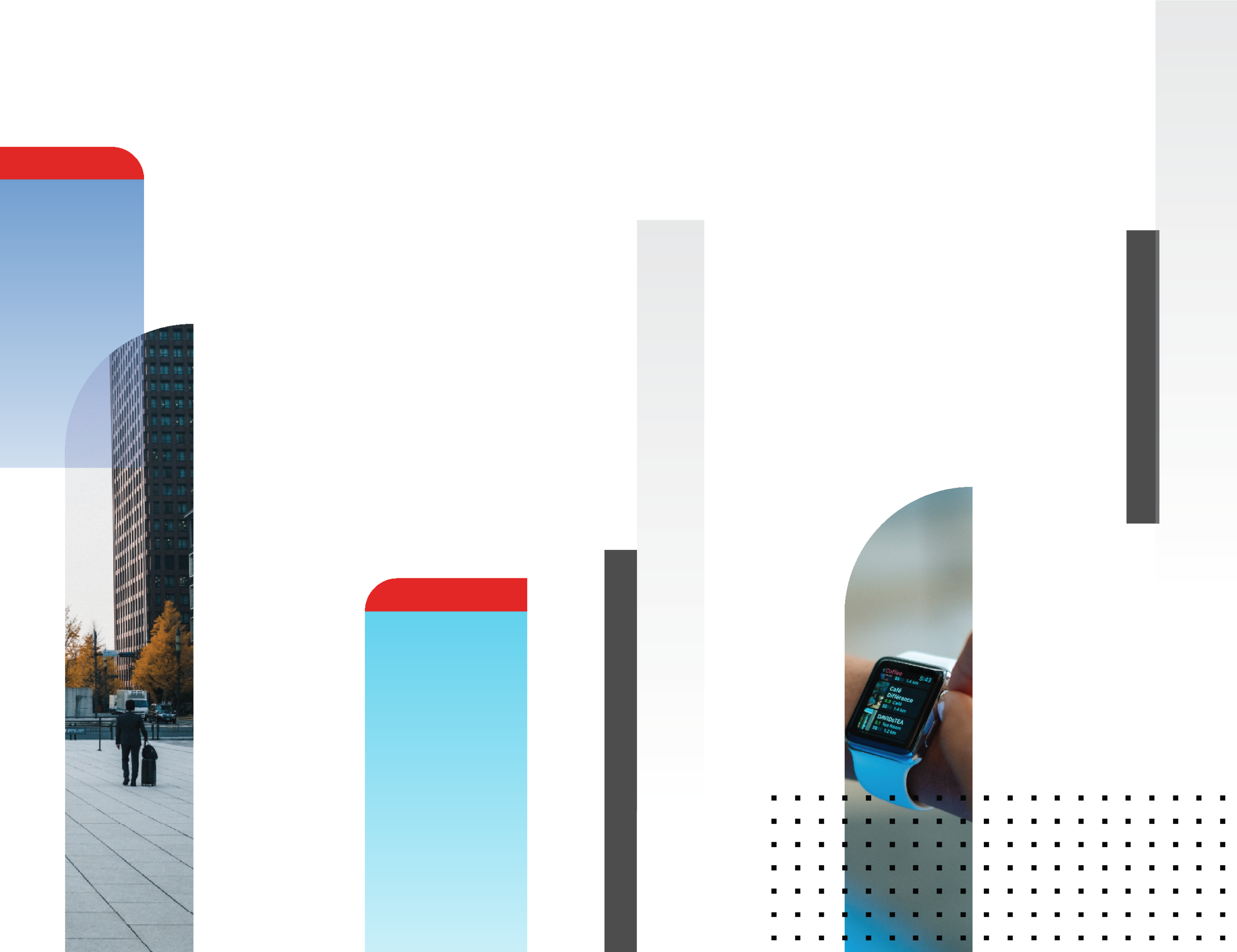
Release Notes

FortiProxy 7.0.5



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

June 17, 2022
FortiProxy 7.0.5 Release Notes
45-705-796179-20220617

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-06-17	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 7.0.5, build 0092:

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:

SSH policy matching

When configuring a firewall policy, the `ssh-policy-check` command has replaced the `ssh-policy-redirect` command.

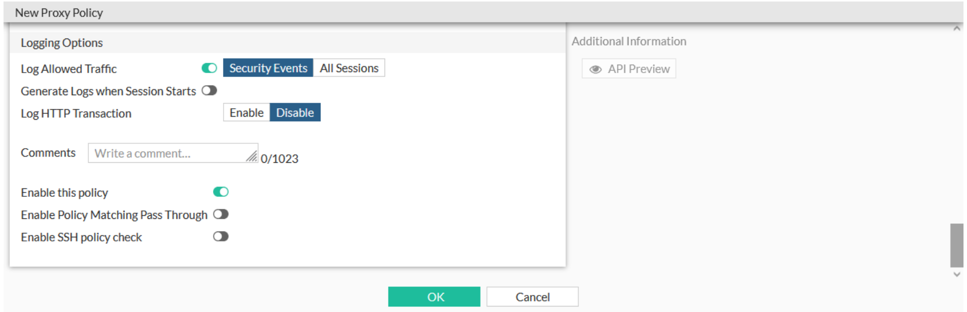
SSH policy check is disabled by default, and can be enabled in transparent and explicit-web policies. When it is enabled, SSH policy matching will only match the SSH policy.

To configure SSH policy check in the CLI:

```
config firewall policy
    edit <policy>
        set ssh-policy-check {disable | enable}
    next
end
```

To configure SSH policy check in the CLI:

1. Go to *Policy & Objects* > *Policy*.
2. Edit a transparent or explicit policy, or create a new policy and set *Type* to *Transparent* or *Explicit*.
3. Enable or disable *Enable SSH policy check*.



New Proxy Policy

Logging Options

Log Allowed Traffic ● [✓ Security Events] All Sessions

Generate Logs when Session Starts ○

Log HTTP Transaction Enable [✓ Disable]

Comments Write a comment... 0/1023

Enable this policy ●

Enable Policy Matching Pass Through ○

Enable SSH policy check ○

4. Click *OK*.

Set CIFS profile in a policy removed

The `cifs-profile` command is removed from the `firewall policy` options.

CIFS can be configure in the GUI by creating or editing a proxy option under *Proxy Settings* > *Proxy Options*, and in the CLI using the `config firewall profile-protocol-options` command:

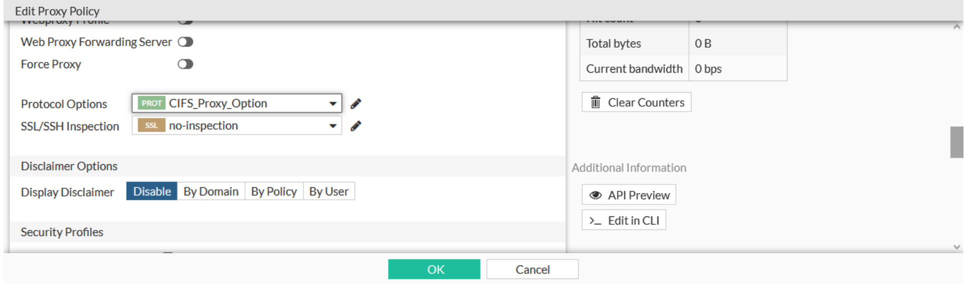
```
config firewall profile-protocol-options
    edit <option>
        config cifs
            set ports <port>
            set status {enable | disable}
            set options <string>
            set oversize-limit <integer>
            set uncompressed-oversize-limit <integer>
            set uncompressed-nest-limit <integer>
            set scan-bzip2 {enable | disable}
            set tcp-window-type {auto-tuning | system | static | dynamic}
            set server-credential-type {none | credential-replication | credential-keytab}
        end
    next
end
```

The proxy option can be then be used in a policy:

- In the CLI, select the option using the set `profile-protocol-options <option>` command:

  ```
  config firewall policy
      edit 1
          set profile-protocol-options <option>
      next
  end
  ```

- In the GUI, select the option in the *Protocol Options* field when editing a policy.



Edit Proxy Policy

Web Proxy Forwarding Server ○

Force Proxy ○

Protocol Options: PROT CIFS_Proxy_Option

SSL/SSH Inspection: SSL no-inspection

Disclaimer Options

Display Disclaimer: [✓ Disable] By Domain By Policy By User

Security Profiles

Total bytes	0 B
Current bandwidth	0 bps

External threat feed through forwarding server

FortiProxy can download external threat feeds as a downstream-proxy in an isolated environment, where the upstream-proxy only has internet access. All SWG functions, including SSL deep-inspection, are performed by the downstream proxy. FDS updates and management is done on the FortiManager.

To configure the external proxy:

```
config system external-resource
    edit <resource>
        set proxy <proxy_server>
        set proxy-port <port>
        set proxy-username <username>
        set proxy-password <password>
    next
end
```

`proxy <proxy_server>`	Proxy server host (IP or domain name).
`proxy-port <port>`	Port number that the proxy server expects to receive HTTP sessions on (1 - 65535, default = 8080).
`proxy-username <username>`	HTTP proxy basic authentication user name.
`proxy-password <password>`	HTTP proxy basic authentication password.

Device ownership CLI command

When device ownership is enabled, ownership enforcement is done at policy level. It is disabled by default.

To enable device ownership:

```
config firewall policy
    edit 2
        set ztna-status enable
        set ztna-ems-tag "FCTEMS_ALL_FORTICLOUD_SERVERS"
        set device-ownership enable
        ...
    next
end
```

Custom virtual host replacement message

Custom messages can be configured for each ZTNA virtual host, to be shown when verification fails. The ZTNA detail tag (`%%ZTNA_DETAIL_TAG%%`) can be included to show the reason for the verification failure.

To use a custom replacement message:

1. Configure a replacement message that includes the ZTNA detail tag in the message:

   ```
   config system replacemsg-group
       edit "test-vhost"
           set comment ''
           set group-type utm
           config webproxy
               edit "ztna-block"
                   set buffer "This is a test message: %%ZTNA_DETAIL_TAG%%"
                   set header http
                   set format html
               next
           end
       next
   end
   ```

2. Apply the replacement message to a virtual host:

   ```
   config firewall access-proxy-virtual-host
       edit "test"
           set host "10.1.200.102"
           set replacemsg-group "test-vhost"
       next
   end
   ```

Proxy policy FTPS handling improvements

To improve FTPS handling in proxy policies:

- When `explicit-ftp-tls` is enabled in the FTP protocol options, FTP is always redirected, regardless of the FTPS status, and deep inspection is done for the explicit FTPS session.

  ```
  config firewall profile-protocol-options
      edit "test"
          config ftp
              set ports 21
              set status enable
              set explicit-ftp-tls {disable | enable}
          end
  ```

```
        next
    end
```

- When deep inspection is enabled, FTPS is always redirected.

SSL options can be configured in SSL/SSH profiles when the protocol is disabled:

```
config firewall ssl-ssh-profile
    edit "no-inspection"
        config ftps
            set status disable
            set client-certificate bypass
            set unsupported-ssl-version allow
            set unsupported-ssl-cipher allow
            set unsupported-ssl-negotiation allow
            set expired-server-cert block
            set revoked-server-cert block
            set untrusted-server-cert allow
            set cert-validation-timeout allow
            set cert-validation-failure block
            set min-allowed-ssl-version tls-1.1
        end
    next
end
```

Forward traffic logs and HTTP transaction logs include the forwardedfor field

The HTTP transaction and Forward session logs include the ClientIP column, that records the client IP address based on the `learn-client-ip` configuration. By default, the `original-source-ip` is recorded.

```
config web-proxy global
    set learn-client-ip {enable | disable}
    set learn-client-ip-from-header {true-client-ip x-real-ip x-forwarded-for}
    set learn-client-ip-srcaddr <address>
    set learn-client-ip-srcaddr6 <address>
end
```

`learn-client-ip {enable	disable}`	Enable/disable learning the client's IP address from headers (default = disable).
`learn-client-ip-from-header {true-client-ip	x-real-ip	x-forwarded-for}`	Learn client IP address from the specified headers: True-Client-IP, X-Real-IP, and X-Forwarded-For.
`learn-client-ip-srcaddr (6) <address>`	Source address name (srcaddr or srcaddr6 must be set).

Display the correct information when doing NTLM authentication

When doing NTLM authentication, the domain is extracted based on the following:

1. If the domain controller has a domain name configured, it is used.
2. Otherwise, if the NTLM type 3 message, from the user, is configured, it is used.
3. Otherwise, if the domain name from the NTLM type 2 message, from the DC, is configured, it is used.

To configure the domain name source, if it is not set:

```
config user domain-controller
    edit "adfs-dc"
        set ip-address 192.168.130.200
        unset domain-name
        set domain-name-src {server | client}
        set ldap-server "adfsldap"
    next
end
```

The domain name can be extracted from either the server's (DC) data, or from the client's data.

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.0.5:

- 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 7.0.5 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 7.0.5.

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

Bug ID	Description
728311	FPX bypassed FTP MODE command when protocol option configuration was set to block.
752001	Route entry removal when `system.ha.unicast-gateway` updates.
781891	The LDAP search filter is lost after upgrading from FortiProxy 2.x to 7.0.
781943	Disable Default Firewall Policy Action for Explicit Proxy on ZTNA rules.
784338	OVF files contain FortiGate-VM references.
785885	Make ZTNA deny traffic log supplies the specific reason (specific tag name, certificate wrong) when a deny happens.
785912	Some fields, such as UTM features, should be hidden according to the policy type, and the `file-filter-profile` field is missing.
787895	WAD crash when updating traffic statistic counters.
787977, 805228	Issues related to the `dedicated-to` option.
789422	Missing ICAP request for CONNECT.
792065	DLP blocks an email with multiple attachments via MAPI, but the log does not show all the blocked files.
794165	TAINTED_SCALAR found in WanOpt_Explicit_Proxy
796019	Access issue with Application Control or IPS.
797270	`ha-mgmt` interface binding issue.
797809	Super_admin is not prompted to select between RO and RW access.
798118	WAD process crashes at `wad_async_queue_time_out`.
799718	When `to-pol` with authentication (group/user) is set to action isolate, the request fails to redirected to WAD and fails to match the given policy in the kernel.
800013, 802841, 807653, 808091, 808203, 808454, 817881, 817995	GUI issues.
800262	When the `auth_type` is not defined inside URL, `"GETURL("auth_type")"` is the NULL pointer. `atoi(NULL)` causes a SEGFAULT making the sslvpnd crash.
801174	Add multiple HTTP request headers and extract .tar.gz file for external resource.

Bug ID	Description
801492	Normal ICAP suddenly becomes abnormal, instantly disconnecting all users. If the ICAP remote server is abnormal, the service connected through FortiProxy will be abnormal.
802222	FSSO traffic log has group information but no user information.
802303	When health check is enabled for a remote ICAP server and then IP address of the remote ICAP server is changed, FortiProxy still does the health check for the old IP address.
802333	When an HTTPS connection policy match fails, it offers an implicit deny or allow policy that does not have a `sec_profile`, so `ssl_opts` is set to NULL. In certain cases this can result in a crash.
802842	Remove `cifs-profile` from `firewall.policy`.
802866	Fix certificate HA synchronization related issues.
803159	The AV UTM log does not cache the correct information when FPX blocks uncompressed oversize file.
803217	When multiple category proxy-address configured in one policy, the URL matches only one destination address category.
803380	When converting explicit web HTTP session to captive portal session, original HTTP session not destroyed, and a new HTTP session is created after handshake.
803452	Fast match flag is changed from enable to disable after changing settings of `profile-protocol-options`.
803794	Custom upgrade code to handle the loss of local certificate data during upgrade
804689	ICAP `respmod-forward-rules` should AND `header-group` entries, not OR.
804853	SSL traffic occasionally fails.
805210	NTLM agentless authentication fails due to user-restriction after FSSO service down.
805819	FPX as explicit web proxy did not block file transfer via ftp-over-http that had the same hash value from ems-threat-feed.
806066	Avoid syncing `outgoing-ip` in `webproxy.global`.
806130	Proxy-address with host-regex match does not match all IP host URLs.
806224	`execute ha manage` does not work for unicast HA in a FortiProxy cluster when a trusted host is configured.
807280	Proxy certificate error when no policy matched.
807332	When HTTP server returns a response header without second CRLF then closes the connection, WAD cannot flush the received data to client.
808040	WAD could not parse the `krb-keytab` with new encryption method.
808043	Explicit proxy policy disclaimer page redirecting to incorrect URL.
808074	Allow content-encoding: UTF-8 passthrough.

Bug ID	Description
808769	Prevent HA syncing of `gui-dashboard` and `ems-tag`.
809813	When doing prefetching, the default 'no inspection' profile is used. In SSL URL filter, a request is exempted when the exempt check is not set.
809813	Prefetch URLsreport crawl for http://www.<whatever>.com failed.
809832	FPX misses local-in rules for NTP server mode.
810179	Traffic shapers applied to the interface are not working as expected.
810570, 811995	Web cache issues.
810571	SSL exempt check condition for non-transparent policies.
811259	Fix WAD leak on IPS session objects.
812897	Remove unused HA session sync (`session-pickup`) commands.
813261	When `learn-client-ip` is enabled, a policy can control based on the IP, but logs do not reflect this.
813317	In transparent mode, `srcaddr-negate`, `dstaddr-negate`, and `service-negate` are available.
813348	Fail to access HTTPS virtual server after the flow control in SSL port improved.
813693	Eventtype `infected` instead of `ems-threat-feed` logged when cached `ems-threat-feed` scan result used in FTP download.
813769	WAD memory leak after enabling ICAP `respmod-forward-rules` profile.
814266	TP policy displays explicit proxy service list, and vice-versa.
814569	Communication between rlogd and miglogd uses a non-standard Netlink protocol.
815203	Masquerade configuration is ignored when L7 address is used in transparent proxy.
815313	WAD crash on `wad_ssl_cert_check_auth_status()`.
816057	Upgrade code for `respmod-forward-rules` header-groups change added.
816205	Uninitialized `ses_ctx usr_addr`.
816913	Source interface in SNAT entry list is empty when it is set to `any`.
817173	IP tables might not be installed properly when the SNAT table contains an FQDN with a wildcard *.
817703	`allow-invalid-server-cert` command available under SSL SSH profile .
817722	When trying to prefetch the same URL twice, the first try succeeds with status code = 0, but the second try fails with status code = 4.
817750	WAD crash when `web-proxy.forward-server-group` does not have `server-list` configured.
817979	When the global web-proxy configuration is changed, the `explicit-outgoing-ip` is not learned, and the daemon continues to use the old `outgoing-ip` address.

Bug ID	Description
818406	304 response if a cached object is generated with Vary headers and is expired.

FORTINET®

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.