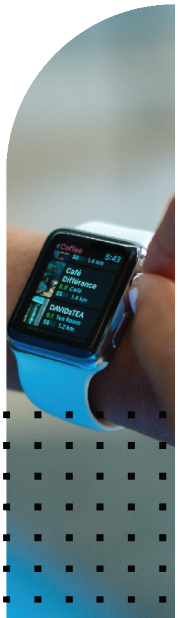
Release Notes

FortiOS 7.0.1



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

March 6, 2024
FortiOS 7.0.1 Release Notes
01-701-721490-20240306

TABLE OF CONTENTS

Change Log **6**
Introduction and supported models **9**
Supported models 9
Special notices **10**
Azure-On-Demand image 10
GCP-On-Demand image 10
ALI-On-Demand image 10
Part numbers of unsupported FG-10xF Generation 2 models 11
Unsupported websites in SSL VPN web mode 11
RDP and VNC clipboard toolbox in SSL VPN web mode 11
CAPWAP offloading compatibility of FortiGate NP7 platforms 11
IP pools and VIPs are not considered local addresses for certain FortiOS versions 12
Changes in CLI **13**
Changes in GUI behavior **19**
Changes in default behavior **20**
Changes in default values **21**
Changes in table size **22**
New features or enhancements **23**
Upgrade information **33**
Fortinet Security Fabric upgrade 33
Downgrading to previous firmware versions 34
Firmware image checksums 35
IPsec interface MTU value 35
HA role wording changes 35
Strong cryptographic cipher requirements for FortiAP 35
How VoIP profile settings determine the firewall policy inspection mode 36
L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later 36
Add interface for NAT46 and NAT64 to simplify policy and routing configurations 37
Upgrading 37
Creating new policies 38
Example configurations 38
Product integration and support **41**
Virtualization environments 41
Language support 42
SSL VPN support 43
SSL VPN web mode 43
Resolved issues **44**
Anti Virus 44
Data Leak Prevention 44

DNS Filter 44
Endpoint Control 44
Explicit Proxy 45
Firewall 45
FortiView 46
GUI 47
HA 49
Intrusion Prevention 50
IPsec VPN 51
Log & Report 52
Proxy 52
REST API 53
Routing 53
Security Fabric 55
SSL VPN 55
Switch Controller 58
System 58
Upgrade 61
User & Authentication 62
VM 62
VoIP 63
WAN Optimization 63
Web Filter 63
WiFi Controller 63
Common Vulnerabilities and Exposures 64
Known issues 65
Endpoint Control 65
Firewall 65
GUI 65
HA 67
IPsec VPN 67
Proxy 68
REST API 68
Routing 68
Security Fabric 69
SSL VPN 69
Switch Controller 69
System 69
User & Authentication 70
VM 70
Built-in AV Engine 71
Resolved engine issues 71

Built-in IPS Engine **72**
Limitations **73**
Citrix XenServer limitations 73
Open source XenServer limitations 73

Change Log

Date	Change Description
2021-07-15	Initial release.
2021-07-16	Updated How VoIP profile settings determine the firewall policy inspection mode on page 36 and Known issues on page 65.
2021-07-20	Updated Changes in CLI on page 13,Changes in GUI behavior on page 19, Changes in default behavior on page 20, Changes in default values on page 21, New features or enhancements on page 23, Resolved issues on page 44, and Known issues on page 65.
2021-07-22	Updated New features or enhancements on page 23, Resolved issues on page 44, and Known issues on page 65. Moved L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later on page 36 and Add interface for NAT46 and NAT64 to simplify policy and routing configurations on page 37 to Upgrade information on page 33.
2021-07-26	Updated New features or enhancements on page 23 and Built-in IPS Engine on page 72.
2021-08-04	Updated Known issues on page 65.
2021-08-09	Updated Changes in CLI on page 13 and Resolved issues on page 44.
2021-08-23	Updated New features or enhancements on page 23, Resolved issues on page 44, Known issues on page 65, and Built-in IPS Engine on page 72.
2021-08-24	Updated Known issues on page 65.
2021-08-30	Updated New features or enhancements on page 23, Resolved issues on page 44, Known issues on page 65, Built-in AV Engine on page 71, and Built-in IPS Engine on page 72.
2021-09-07	Updated Resolved issues on page 44 and Known issues on page 65.
2021-09-20	Updated New features or enhancements on page 23, Resolved issues on page 44, Known issues on page 65, and Built-in AV Engine on page 71.
2021-10-04	Updated Resolved issues on page 44 and Known issues on page 65.
2021-10-05	Updated L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later on page 36.
2021-10-19	Updated Resolved issues on page 44, Known issues on page 65, and Built-in AV Engine on page 71.
2021-10-22	Updated Part numbers of unsupported FG-10xF Generation 2 models on page 11.
2021-10-25	Updated Changes in CLI on page 13, New features or enhancements on page 23, Resolved issues on page 44, and Known issues on page 65.
2021-11-01	Updated Resolved issues on page 44 and Known issues on page 65.
2021-11-15	Updated Known issues on page 65.

Date	Change Description
	Added Unsupported websites in SSL VPN web mode on page 11.
2021-11-24	Updated Fortinet Security Fabric upgrade on page 33 and Product integration and support on page 41.
2021-11-29	Updated Resolved issues on page 44 and Known issues on page 65.
2021-12-02	Updated Resolved issues on page 44 and Known issues on page 65.
2021-12-13	Added RDP and VNC clipboard toolbox in SSL VPN web mode on page 11. Updated Changes in CLI on page 13 and Resolved issues on page 44.
2022-01-10	Updated Known issues on page 65.
2022-01-24	Updated Changes in default behavior on page 20 and Known issues on page 65.
2022-02-03	Updated New features or enhancements on page 23 and Known issues on page 65.
2022-02-07	Updated Known issues on page 65.
2022-02-22	Updated Changes in CLI on page 13 and Known issues on page 65.
2022-03-07	Updated Known issues on page 65.
2022-04-01	Updated Resolved issues on page 44 and Known issues on page 65.
2022-05-10	Added CAPWAP offloading compatibility of FortiGate NP7 platforms on page 11. Updated Resolved issues on page 44.
2022-05-12	Updated Introduction and supported models on page 9.
2022-06-09	Updated L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later on page 36.
2022-06-16	Updated L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later on page 36 and Add interface for NAT46 and NAT64 to simplify policy and routing configurations on page 37.
2022-06-27	Updated Resolved issues on page 44.
2022-08-15	Updated Resolved issues on page 44 and Known issues on page 65.
2022-10-03	Updated Known issues on page 65.
2022-10-17	Updated Known issues on page 65.
2022-10-24	Updated Known issues on page 65.
2022-11-02	Updated Known issues on page 65.
2022-12-16	Updated New features or enhancements on page 23.
2023-01-20	Updated New features or enhancements on page 23.
2023-01-27	Updated Known issues on page 65.
2023-02-22	Updated Resolved issues on page 44.

Date	Change Description
2023-03-06	Updated Changes in default behavior on page 20 and Known issues on page 65.
2023-03-10	Updated Resolved issues on page 44.
2023-03-23	Updated Changes in default behavior on page 20 and Resolved issues on page 44.
2023-04-17	Updated Known issues on page 65.
2023-05-03	Updated How VoIP profile settings determine the firewall policy inspection mode on page 36 and Known issues on page 65.
2023-05-15	Updated Known issues on page 65.
2023-06-13	Added IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 12. Updated Changes in default behavior on page 20.
2023-08-21	Updated Changes in CLI on page 13.
2023-09-06	Updated Built-in IPS Engine on page 72.
2023-10-17	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 12.
2023-12-27	Updated Resolved issues on page 44.
2024-02-13	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 12.
2024-03-06	Updated Known issues on page 65.

Introduction and supported models

This guide provides release information for FortiOS 7.0.1 build 0157.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.1 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-81E, FG-81E-POE, FG-81F, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

See Part numbers of unsupported FG-10xF Generation 2 models on page 11 for more information about the FG-100F and FG-101F models.

Special notices

- Azure-On-Demand image on page 10
- GCP-On-Demand image on page 10
- ALI-On-Demand image on page 10
- Part numbers of unsupported FG-10xF Generation 2 models on page 11
- Unsupported websites in SSL VPN web mode on page 11
- RDP and VNC clipboard toolbox in SSL VPN web mode on page 11
- CAPWAP offloading compatibility of FortiGate NP7 platforms on page 11
- IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 12

Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

Part numbers of unsupported FG-10xF Generation 2 models

The following part numbers are Generation 2 models that do not support FortiOS 7.0.1:

- FG-100F-Gen2 P24589-20
- FG-101F-Gen2 P24605-20

Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1 and later:

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1 and later.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms running FortiOS 7.0.1 and later, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

IP pools and VIPs are not considered local addresses for certain FortiOS versions

For FortiOS 6.4.9 and later, 7.0.1 to 7.0.12, 7.2.0 to 7.2.5, and 7.4.0, all IP addresses used as IP pools and VIPs are not considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is not considered a destination for those IP addresses and cannot receive reply traffic at the application layer without special handling.

- This behavior affects FortiOS features in the application layer that use an IP pool as its source IP pool, including SSL VPN web mode, explicit web proxy, and the phase 1 local gateway in an interface mode IPsec VPN.
- The FortiGate will not receive reply traffic at the application layer, and the corresponding FortiOS feature will not work as desired.
- Configuring an IP pool as the source NAT IP address in a regular firewall policy works as before.

For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

Changes in CLI

Bug ID	Description
550819	Rewrite RDP and VNC handling. The following commands have been added: • Add color depth under VNC bookmark entry. `config vpn ssl web portal` `edit <name>` `config bookmark-group` `edit <name>` `config bookmarks` `edit <name>` `set apptype vnc` `set color-depth {32 | 16 | 8}` `set logon-user <string>` `next` `end` `next` `end` `next` `end` `config vpn ssl web {user-group-bookmark user-bookmark}` `config bookmarks` `edit <name>` `set apptype vnc` `set color-depth {32 | 16 | 8}` `set logon-user <string>` `next` `end` `end` • Add color depth, restricted administrator, send pre-connection ID, and keyboard layout under RDP bookmark entry. `config vpn ssl web portal` `edit <name>` `config bookmark-group` `edit <name>` `config bookmarks` `edit <name>` `set apptype rdp` `set color-depth {32 | 16 | 8}` `set restricted-admin {enable | disable}` `set send-preconnection-id {enable | disable}`

Bug ID	Description

```
                        set keyboard-layout <option>
                    next
                end
            next
        end
    next
end

config vpn ssl web {user-group-bookmark user-bookmark}
    config bookmarks
        edit <name>
            set apptype rdp
            set color-depth {32 | 16 | 8}
            set restricted-admin {enable | disable}
            set send-preconnection-id {enable | disable}
            set keyboard-layout <option>
        next
    end
end
```

- Add web mode RDP and VNC clipboard control.

```
config vpn ssl web portal
    edit <name>
        set clipboard {enable | disable}
    next
end
```

The following commands have changed:

- Change maximum value for pre-connection ID under all RDP bookmark entries.

```
config vpn ssl web portal
    edit <name>
        config bookmark-group
            edit <name>
                config bookmarks
                    edit <name>
                        set apptype rdp
                        set preconnection-id <integer, 0 - 4294967295>
                    next
                end
            next
        end
    next
end

config vpn ssl web {user-group-bookmark user-bookmark}
    config bookmarks
        edit <name>
```

Bug ID	Description
	`` set apptype rdp set preconnection-id <integer, 0 - 4294967295> next end end ``` The following commands have been removed: • Remove `server-layout` attribute under all RDP bookmark entries. • Remove unsupported application types (`citrix` and `portforward`) from all bookmark entries for `allow-user-access` attribute. • Remove `diagnose app guacd` debug command.
585899	Add `management-port-use-admin-sport` option under `config system global` to enable/disable using the `admin-sport` as management port. If disabled, allow specifying the `management-port`. ``` config system global set management-port-use-admin-sport {enable | disable} end ```
630083	Add `traceroute` option to use SD-WAN rules for output interface. ``` # execute traceroute-options use-sdwan Use SDWAN rules to get output interface <yes | no>. ```
674576	Extend CRL verification options (formerly `strict-crl-check`) to include CRL expiry, leaf absence, and chain absence in certificate verification. If any of the CRL verification options are enabled upon revoke, the certificate status will be marked as revoke. ``` config vpn certificate setting config crl-verification set expiry {ignore | revoke} set leaf-crl-absence {ignore | revoke} set chain-crl-absence {ignore | revoke} end end ``` The default setting for each option is ignore.
687486	Move configuration option for `youtube-restrict` from `videofilter profile` back to `webfilter profile`.
687833	Introduce a new DNS server selection method and CLI option to change how configured DNS servers are prioritized. The server-select-method option specifies how configured servers are prioritized, either based on least round-trip time (`least-rtt`) or the order they are configured (`failover`). Alternate primary and secondary DNS servers can be configured, but they are not used as failover DNS servers. ``` config system {dns vdom-dns} set server-select-method {least-rtt | failover} set alt-primary <class_ip> set alt-secondary <class_ip> ```

Bug ID	Description
	`end`
688989	Change `username-case-sensitivity` option to `username-sensitivity`. This new option includes both case sensitivity and accent sensitivity. When disabled, both case and accents are ignored when comparing names during matching. `config user local` `edit <name>` `set username-sensitivity {enable | disable}` `next` `end`
693347	Restrict IPv6 pools address and IPv6 split tunneling routing address to be IP mask or range type only so SSL VPN can support EMS tag dynamic addresses. `config vpn ssl web portal` `edit <name>` `set ipv6-pools <address>` `set ipv6-split-tunneling-routing-address <address>` `next` `end`
696675	Update the options for the `auto-scale` role: `config system auto-scale` `set role {primary | secondary}` `end`
697566	Allow ip_no_pmtu_disc to be set manually under `config system global` by adding am option to configure PMTU discovery. This value will set the kernel value for ip_no_pmtu_disc (default = 1). `config system global` `set pmtu-discovery {enable | disable}` `end`
700840	Add support for IPv6 VRF. `config router bgp` `config vrf-leak6` `edit <vrf>` `config target` `edit <vrf>` `set route-map <string>` `set interface <string>` `end` `end` `next` `end` The VRF origin and target IDs are an integer between 0 - 31. `config router static6`

Bug ID	Description
	`` edit <id> set vrf <integer> next end ``` The VRF is an integer between 0 - 31.
704624	Move the `delay` and `required` settings from the `automation-action` table to the `automation-stitch` table within an `actions` subtable so they can be set per stitch. ``` config system automation-stitch edit <name> set trigger <name> config actions edit 1 set action <name> set delay <integer> set required {enable | disable} next edit 2 set action <name> next end next end ```
709109	Add the following option to backup configuration files using SFTP: ``` # execute backup config sftp <file name> <SFTP server><:SFTP port> [user] [password] ```
710125	Add support for static, round-robin, weighted, first alive, and HTTP host load-balancing methods to have hold down option to the real server of the access proxy. ``` config firewall access-proxy edit <name> config api-gateway edit <id> config realservers edit <id> set ip <address> set port <integer> set status active set health-check enable set holddown-interval {enable | disable} set health-check-proto {ping | http | tcp-connect} next end next end ```

Bug ID	Description
	`next` `end` The `holddown-interval`option is only available if the real server health check of the access proxy is enabled.
710730	Update antivirus quarantine settings to reflect that they are now based on machine learning malware detection instead of heuristics. `config antivirus quarantine` `set drop-machine-learning <option>` `set store-machine-learning <option>` `end`
711484	Add certificate authentication support for proxy policy authentication. `config authentication setting` `set cert-auth {enable | disable}` `set cert-captive-portal <hostname>` `set cert-captive-portal-ip <address>` `set cert-captive-portal-port <integer>` `end` Where `cert-captive-portal-port` is the captive portal port number (1 - 65535, default = 7832).
712794	Allow the wireless controller to obtain temperature values from FortiAP-F models that have built-in temperature sensors: `# diagnose wireless-controller wlac -c wtp <serial number> | grep Temp`

Changes in GUI behavior

Bug ID	Description
641052	Add multi-select mode on *Local Out Routing* page to allow multiple local out settings to be configured together.
690425	Add global search option in the GUI for users to search for keywords appearing in objects and navigation menus to quickly access the object and configuration page.
695284	Add support for displaying ADVPN shortcut tunnel information in the *SD-WAN* and *IPsec* dashboard widgets.
708810	A FortiToken Cloud license can now be purchased through FortiExplorer. In the FortiGate GUI, enhancements help customers to easily download the FortiExplorer app. Clear warning messages are added to indicate if there is no FortiToken Cloud subscription, or the subscription is expired. The default token type when enabling two-factor authentication has changed to FortiToken Cloud.

Changes in default behavior

Bug ID	Description
655991	Consolidates multiple NAT46/NAT64 related objects into regular objects, and introduce a per-VDOM virtual interface, `naf.<vdom>`, that is automatically added to process NAT46/NAT64 traffic. The new changes and additions include: • Consolidate `vip46` and `vip64` setting into `vip` and `vip6` configurations. • Consolidate `policy46` and `policy64` settings into `firewall policy` settings. • Introduce `nat46`/`nat64` in `firewall policy` settings. • Extend `ippool` and `ippool6` to support NAT46 and NAT64. • Extend central SNAT to support NAT46 and NAT64. • Remove `firewall vip46`/`vip64`, `vipgrp46`/`vipgrp64`, and `policy46`/`policy64` settings. • Rename `system.nat64` to `system.dns64`. To configure NAT46/NAT64 translation, users can use the standard `vip`/`vip6` setting, apply it in a firewall policy, enable NAT46/NAT64, and enter the IP pool to complete the configuration.
699533	In FortiOS 7.0, the default authentication protocol for a switch controller SNMP user is SHA256, as opposed to the default SHA1 in previous versions.
709056	Previously, the `tie-break fib-best-match` option in SD-WAN service rules selected the outgoing interface between all links that has a valid route to the destination. In this update, the option is extended to consider only the best routes. This works on manual, priority, and SLA SD-WAN service modes. The longest match routes will override the quality comparisons when all of the specific routes are out of SLA. This applies to priority and SLA SD-WAN rules.
709391	The link monitor health check for access proxy real servers had been added for ZTNA. This enhancement will deploy the server health check status to the WAD daemon. • Add server health check status (`ALIVE/DIE`) to the `wad_vs_server`. • Query the link monitor health check status when creating the `wad_vs_server`. • When the link monitor health check status changes, the generation in the CMDB debug zone is updated. • WAD daemon updates the `wad_vs_server` health check status when a generation change is detected.
714831	Remove related ZTNA tags when an EMS connection is deleted from Fabric connector.
717170	The interface TCP MSS setting now applies to RX and TX TCP MSS.
718512	Allow policy route match in the reply direction, and improve IPv6 route search for policy route to keep the same behavior as IPv4.
718571	DHCP relay interfaces are released/initialized for added/deleted relay interfaces only. All other relay interfaces will remain unchanged. All DHCP relay interfaces now share one socket instead of one socket per interface. Additionally, DHCP relay now listens on the Layer 3 socket. If customers are using local-in policies to deny any/all traffic, they must create an accept policy to allow UDP/67 traffic before the deny policy, since the FortiGate will now block these packets on the Layer 3 socket.

Changes in default values

Bug ID	Description
708351	Change default value of ZTNA `firewall.access-proxy.empty-cert-action` to `block`.
712671	Change access proxy API gateway real server default port from 0 to 443. `config firewall access-proxy` `edit <name>` `set vip <string>` `config api-gateway` `edit <id>` `config realservers` `edit <id>` `set port <integer>` `next` `end` `next` `end` `next` `end` Where the `port` is a value from 1 - 65535 (default = 443).

Changes in table size

Bug ID	Description
662615	FG-80F series supports a total of 96 WTP entries (normal 48).
699766	Increase system DNS database table size from 256 per VDOM and 512 global to 1024 per VDOM and unlimited global.
712616	Increase firewall service custom table size from 16,384 per VDOM to 32,768 on FG-3000 series models and higher.
713686	Increase router `static6` table size from 500 per VDOM to 2000 per VDOM on FG-600-series models and higher.
713695	Increase central NAT rules (`firewall.central-snat-map`) on 1U platforms from 1024 to 2048.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
477886	Allow ingress and egress ports to be configured so the PRP trailer is not stripped when PRP packets come in or go out. `config system npu` `set prp-port-in <port>` `set prp-port-out <port>` `end`
489956	Add LAG implementation so each session uses the same NP6 and XAUI for ingress and egress directions to avoid fast path congestion (this setting is disabled by default). `config system npu` `set lag-out-port-select {enable | disable}` `end` Add algorithm in NPU driver for distribution, `AGG_ALGORITHM_NPU`.
568534	The DHCP snooping server access list allows servers on that list to respond to DHCP requests, while blocking requests to servers that are not on the list. The DHCP server access list feature can be enabled from the VDOM or switch level. Server lists are configured per switch VLAN interface. VDOM level: `config switch-controller global` `set dhcp-server-access-list {enable | disable}` `end` FortiSwitch level: `config switch-controller managed-switch` `edit <switch>` `set dhcp-server-access-list {global | enable | disable}` `next` `end` Interface: `config system interface` `edit <interface>` `config dhcp-snooping-server-list` `edit <list>` `set server-ip <class_ip>` `next` `end` `next` `end`

Bug ID	Description
575686	When configuring an SSID in bridge mode, users can select individual security profiles instead of a security profile group. This applies to models in the FAP-U series that can perform UTM on the FortiAP itself.
613092	Allow SSL VPN to be explicitly enabled or disabled from the GUI and CLI. To connect, SSL VPN must be enabled and the SSL VPN interface must be up. `config vpn ssl settings` `set status {enable | disable}` `end`
658039	Add CLI option `set auto-discovery-shortcut-mode` in the OCVPN configuration to control if shortcuts should be torn down when the parent tunnel is down. This option is only available on the primary hub, and is shared with spokes via the cloud. Setting this option in the OCVPN configuration will cause the generated `phase1-interface` object to set its `auto-discovery-shortcuts` option. `config vpn ocvpn` `set auto-discovery-shortcut-mode {independent | dependent}` `end`
669942	In the scenario where session synchronization is down between two FGSP members that results in a split-brain situations, the IKE monitor provides a mechanism to maintain the integrity of state tables and primary/secondary roles for each gateway. It continues to provide fault tolerance by keeping track of the timestamp of the latest received traffic, and it uses the ESP sequence number jump ahead value to preserve the sequence number per gateway. Once the link is up, the cluster resolves the role and synchronizes the session and IKE data. During this process, if the IKE fails over from one unit to another, the tunnel will remain valid due to the IKE session and role being out of sync, and the ESP anti-replay detection.
670058	Conventionally, public cloud FortiGate deployments require four NICs (external data processing, internal data processing, heartbeat/synchronization, and HA management). The HA heartbeat and management have been merged into the same interface, so only three NICs are required.
687892	Add replacement message for video filter and show block reason (video category or channel). `config videofilter profile` `edit <profile>` `set replacemsg-group <profile_name>` `next` `end`
689139	Add shortcuts to various locations in the GUI to help users register their FortiGate to FortiCare. This option is also added to newly authorized Fabric FortiGates.
689931	With NAC LAN segment support, the VLAN segmentation is handled by the FortiSwitch. Devices can maintain the same IP that they initially receive while onboarding. When a NAC policy is matched, the device gets placed into the appropriate VLAN by the FortiSwitch, providing segmentation from other LAN segments.

Bug ID	Description
690671	Filtering PFCP traffic is supported on FortiOS Carrier. PFCP filtering is required to provide security for evolving 4G networks and upcoming 5G networks. PFCP filtering is configured similar to GTP filtering. PFCP message filters and profiles are created and applied in firewall policies.
692529	Enhance MAC authentication bypass so that the MAC authentication status is recorded in authd. The MAC authentication is retired in 10 seconds and is always sent to the portal for HTTP authentication sessions.
696057	Add REST API to retrieve a list of FortiSwitch models that are supported on the FortiGate: `/api/v2/monitor/switch-controller/managed-switch/models`
696844	In central NAT mode, allow VIPs to have a status option to enable or disable its status.
697340	When indoor AP models are placed outdoors, or outdoor AP models are placed indoors, there is an option to override the indoor or outdoor flag. This enables the available channels list to reflect the region based on the AP placement.
697843	On models that have an internal switch that supports modifying the distribution algorithm, enhanced hashing can be used to help distribute traffic evenly across links on the LAG interface. The enhanced hashing algorithm is based on a 5-tuple of the IP protocol, source IP address, destination IP address, source port, and destination port. The computation method can also be specified.
699006	On a FortiCarrier, the new RAT (radio access technology) timeout profile allows users to customize the timeout values for each RAT type. This profile can be applied to GTP profiles to allow GTP tunnel timeout per RAT type (default value is 0 seconds).
699205	Add dynamic firewall address subtype, *Switch Controller NAC Policy Tag*. This type of address can be assigned to a NAC policy under *Switch Controller Action*. All device MACs discovered in the NAC policy will be added to the firewall address dynamically.
699226	Add `diagnose switch-controller switch-info port-properties [<switch>] [<port>]` command to display FortiSwitch port properties, such as PoE power level, connector module form factor, and speed capabilities. `# diagnose switch-controller switch-info port-properties S548DF**********` `Switch: S548DF**********` `Port: port1` `PoE : 802.3af/at,30.0W` `Connector : RJ45` `Speed : 10Mhalf/10Mfull/100Mhalf/100Mfull/1Gauto/auto`
699268	Add realm support on FortiGate SSL VPN client. `config vpn ssl client` `edit <client>` `set realm <string>` `next` `end`
699456	Increase the generated RSA key bits from 1024 to 2048.
700073	Add a default-action into `youtube-channel-filter` configuration to apply a default action to all channels when there is no match.

Bug ID	Description
	config videofilter youtube-channel-filter edit <id> set default-action {block | monitor | allow} set log {enable | disable} next end The default settings are monitor for default-action, and disable for log.
700665	Allow FortiAI to be used with antivirus profiles in proxy inspection mode. FortiAI inspects high-risk files and issues a verdict to the firewall based on how close a file's features match those of malware. When enabled, FortiAI can log, block, or ignore the file based on the verdict.
701033	Support octets and MAC address formats in SNMP engine ID configuration that are defined in RFC-2571. config system snmp sysinfo set engine-id-type {text | hex | mac} set engine-id <string, maximum 27 characters> end
702665	Add support for BGP conditional advertisement for IPv6 on the FortiGate: config router bgp config neighbor edit <name> config conditional-advertise6 edit <name> set condition-routemap <string> set condition-type {exist | non-exist} next end next end end
703312	Improve switch controller performance in large topologies.
703900	In an SD-WAN transit routing setup with Google Network Connectivity Center (NCC), you can route data and exchange border gateway protocol (BGP) routing information between two or more remote sites via GCP.
704318	Add SNMP OIDs to query FortiSwitch CPU, memory, and port status via the FortiGate. These objects are added to the FortiOS enterprise MIB 2 tables.
704662	Allow the FortiGate to use the built-in speed test functionality to dynamically populate egress bandwidth to individual dial-up tunnels from the hub. Changes include: • Allow upload speed tests to be run from the hub to spokes for dial-up IPsec tunnels. • Allow an SD-WAN member on a spoke to switch routes when speed test is being run from the hub to spokes. • Allow speed test result to be applied dynamically on dial-up IPsec tunnel interface for egress

Bug ID	Description
	traffic shaping. • Allow traffic shaping profile to be applied on dial-up IPsec tunnel interface on the hub. • Add the ability to apply class ID and percentage based QoS settings to individual child tunnels using a traffic shaping policy and profile.
704819	Using the RADIUS attribute Tunnel-Private-Group-Id, a wireless controller can now accept a VLAN name as a string, and match the VLAN sub-interface attached to a VAP interface when dynamically assigning a VLAN. Users logging into an SSID can be dynamically assigned to the proper VLAN based on the VLAN configurations on RADIUS for the particular user.
706491	On FortiClient EMS versions that support `push CA certs` capability, the FortiGate will push CA certificates used in SSL deep inspection to the EMS server. On the EMS server, the CA certificates can be selected in the managed endpoint profiles so they can be installed on managed endpoints.
707143	NetFlow and SFlow now support using SD-WAN in `interface-select-method` for selecting the outgoing interface. `config system {netflow sflow vdom-netflow vdom-sflow}` `set interface-select-method {auto | sdwan | specify}` `set interface <interface>` `end`
707388	EMS shares `Is_online information` with the FortGate, which is used to decide whether the FortiGate will allow the traffic by the ZTNA access proxy policy.
707475	Enhancements for ZTNA logging: • Add ZTNA log subtype to UTM logs. • Six scenarios will generate allow and deny logs in the new ZTNA category. • Add traffic log ID for ZTNA related traffic.
707643	Implement best route mode for SD-WAN rules, including ECMP support for the longest match and the longest match overriding the quality comparison.
708358	Passive health check for SD-WAN can be configured in the GUI from two locations: 1. *Network* > *SD-WAN* > *Performance SLA* tab: probe mode options are *Active*, *Passive*, or *Prefer Passive*. The disabled option can only be configured in the CLI. 2. In a *Firewall Policy* where the destination is a SD-WAN zone, the passive health check option is available. By enabling *Passive Health Check* in a policy, the TCP traffic for that policy will be used in health check measurements.
709061	In *WiFi & Switch Controller* > *Managed Switch* > *Topology View*, a new *Reorder* button provide users with the ability to rearrange the order that the FortiSwitches appear.
709067	Add support for RFC 5709 HMAC-SHA cryptographic authentication for OSPF: `config router key-chain` `edit <name>` `config key` `edit <id>` `set algorithm {md5 | hmac-sha1 | hmac-sha256 | hmac-sha384 | hmac-sha512}`

Bug ID	Description
	next end next end
709090	The FortiWiFi mesh function supports obtaining Fortinet MAC OUI ranges from the FortiGuard MAC address database (MADB), so that leaf FortiAPs with new MAC OUIs can be automatically recognized and allowed.
709104	WANOpt supports SSL offloading of traffic without needing to define an SSL server. The server side FortiGate will re-sign the HTTP server's certificate without needing to configure an SSL server (in both scenarios where an external proxy is and is not used). This enhancement also adds support for GCM cipher and ChaCha ciphers in the SSL connection.
709107	Allow FortiGate to support client certificate authentication used in mTLS communication between client and server. In this communication, clients are issued certificates by the CA. An access proxy configured on the FortiGate may use the new certificate method in the authentication scheme to identify and approve the client certificate provided by the client when it tries to connect to the access proxy. Optionally, the FortiGate may add the HTTP header `X-Forwarded-Client-Cert` to forward the certificate information to the server.
709108	The TCP forwarding access proxy supports communication between the client and access proxy without SSL/TLS encryption. The connection between the client and access proxy still begins with a TLS handshake. The client uses the HTTP 101 response to switch protocols and remove the HTTPS stack. Further end-to-end communication between the client and server is encapsulated in the specified TCP port, but otherwise not encrypted by the access proxy.
710318	Add security rating test in *Access Control and Authentication* to mitigate against the following high-priority vulnerability: • LDAP Server Identity Check: ensures certificate validation takes place against LDAP server.
710323	Add security rating test in *Access Control and Authentication* to mitigate against the following high-priority vulnerability: • Disable Username Case-Sensitivity Check: ensures users cannot bypass two-factor authentication by using a different case than configured in the user object.
710423	When connecting to FortiAnalyzer in the Security Fabric, the FortiGate displays an *Authorize* button when the FortiGate has not be authorized on the FortiAnalyzer side. This opens a shortcut to log in to the FortiAnalyzer and approve the FortiGate.
711577	Add warnings to inform users when an installed firmware is not signed by Fortinet. The warning message appears in the CLI when the uploaded firmware fails signature validation, and when logging in to the FortiGate from the GUI. Additional messages are added in various places once a user is logged in to the GUI to remind them of the unsigned firmware.
711868	FortiTester can be added to the Security Fabric and authorized from the Security Fabric topology view. Once added, the FortiTester appears in the dashboard Security Fabric widget, and it can be added to the dashboard as a Fabric device widget.
712102	The REST API can retrieve dynamic information about LTE modems, such as RSSI signal strength, SIM information, data session, and usage levels from 3G and 4G FortiGates.

Bug ID	Description
712304	Support new Google gVNIC interface, which offers improved performance and bandwidth and is required in some VM shapes that are tuned for optimal performance.
712916	SD-WAN zones can be applied in three new ways: **1.** Use the SD-WAN zone in IPv4 and IPv6 static routes. **2.** Use the SD-WAN zone in SD-WAN service rules. **3.** Add a pre-defined SD-WAN zone called SASE. The following commands are added: `config router {static | static6}` `edit <id>` `set sdwan-zone <string>` `next` `end` `config system sdwan` `config service` `edit <id>` `set priority-zone <string>` `next` `end` `end` The following commands are removed: `config router {static  static6}` `edit <id>` `set sdwan {enable | disable}` `next` `end`
713011	When a FortiGate has multiple EMS entries configured, instead of querying every EMS server to fetch device information for device certificate validation, add optional EMS server information for WAD device query to fcnacd. This allows fcnacd to direct the query for the device only to the specific EMS.
713535	Sniffer traffic logs from the IPS engine are expanded to 64-bit variable sizes (previously 32-bit for sent/received bytes fields).
713690	Add user count per LDAP group in an Active Directory. When LDAP users log on through firewall authentication, the active users per LDAP group is counted and displayed in the *Firewall Users* view and CLI.
713717	The FortiGate can automatically downgrade to use TLS version 1.2 when there are no proper custom ciphers configured in TLS 1.3 in a server load-balance VIP configuration.
713793	Allow FortiGates to read the Cisco Security Group Tag (SGT) in Ethernet frames and use them as matching criteria in firewall policies. A policy can match based on the presence of an SGT, or the detection of a specific ID or IDs. This feature is available in flow mode policies for virtual wire pair policies or policies in transparent mode VDOMs.

Bug ID	Description
714713	Allow SSL VPN interfaces to be used in zones.
715031	Add option in the SSL VPN web portal profile to disable the use of the copy and paste clipboard in RDP and VNC connections while using web mode.
715100	Allow FortiClient to use a browser as an external user agent to perform SAML authentication for SSL VPN tunnel mode. In prior versions, SAML authentication must be performed within the FortiClient embedded login window. A new setting is added to configure the SAML redirection port upon successful SAML authentication: `config vpn ssl settings` `set saml-redirect-port <port>` `end`
716453	On KVM, FortiOS can support bootstrapping using a MIME file via config drive.
716683	FIPS CC mode is now supported on OCI and GCP FortiGate VMs. `config system fips-cc` `set status fips-ciphers` `end` To enable this feature, all VPNs must be removed.
717336	The dedicated management CPU feature ensures that CPU 0 is only used for management traffic. This feature, which was previously available for 2U models and higher, is now available on 1U models.
717579	Add command in the WTP profile to disable console login from the FortiAP: `config wireless-controller wtp-profile` `edit <profile>` `set console-login {enable | disable}` `next` `end` All managed APs using this profile will be rebooted and changes will be applied.
717591	For SSIDs in local standalone NAT mode, add the option to define up to three DNS servers to assign to wireless endpoints through DHCP.
717907	Add option in CLI to manage how long authenticated FSSO users on the FortiGate will remain on the list of authenticated FSSO users when a network connection to the collector agent is lost: `config user fsso` `edit <name>` `set logon-timeout <integer>` `next` `end` The `logon-timeout` is measured in minutes (1 - 2880, default = 5).

Bug ID	Description
719581	Allow the FortiGate to use the built-in speed test functionality to dynamically populate egress bandwidth to individual dial-up tunnels from the hub. It allows the speed test results of dial-up tunnels to be cached for reuse when the tunnel is up again.
719764	Allows IPv6 to be configured in several ZTNA scenarios: • IPv6 client with IPv6 server • IPv6 client with IPv4 server • IPv4 client with IPv6 server Configuration changes include: • Add `access-proxy` type in `firewall.vip6` • Add `firewall.access-proxy6` • Add `firewall.access-proxy(6).api-gateway6` • Add `access-proxy6` in `firewall.proxy-policy`
720046	Add option to toggle between enabling or disabling policy route updates when a link monitor fails. By disabling policy route updates, a link monitor failure will not cause corresponding policy based routes to be removed.
720136	When configuring a radio in service assurance management (SAM) mode, support is added to configure the client to authenticate with the captive portal. The captive portal match string, success string, and failure string must be specified to automatically detect the authentication success or failure.
720723	The link monitor can configure multiple servers and allow each server to have its own weight setting. If the link monitor is down, it will trigger static route updates and cascade interface updates if the weight of all dead servers exceeds the monitor's fail weight threshold.
721280	New options are added to the SSL/SSH profile to log server certificate information and TLS handshakes. New fields are added to the UTM SSL logs when these options are enabled.
721798	When a FortiGate FGCP HA active-passive cluster fails over, CAPWAP traffic is able to quickly fail over to a secondary device, which prevents significant AP downtime with minimal impact for wireless clients. CAPWAP hitless failover with FGCP is only available on FortiAP AX platforms and F-series models when FortiGates are running in active-passive mode.
722649	ZTNA can be configured with an SSH access proxy to provide a seamless SSH connection to the server. The advantages of an SSH access proxy over a TCP forwarding access proxy include: • Establishing device trust context with user identity and device identity checks • Applying SSH deep inspection to the traffic through an SSH related profile • Performing optional SSH host key validation of the server • Having one-time user authentication to authenticate the ZTNA SSH access proxy and SSH server connections
723176	Support logging for FortiGate generated local out DNS traffic. A new setting is added for the local DNS log: `config system dns` `  set log {disable | error | all}` `end`

Bug ID	Description
723178	When a user disconnects from an IPsec VPN tunnel, it is sometimes not desirable for the released IP to be immediately used up in the current first available IP assignment method. A new setting is added to hold an IP for a delay interval in seconds (0 - 28800) before it is released for use. IPs are still assigned by the first available method. `config vpn ipsec phase1-interface` `edit <name>` `set ip-delay-interval <integer>` `next` `end`

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 7.0.1 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.0.1
FortiManager	• 7.0.1
FortiClient* Microsoft Windows	• 7.0.0 build 0029
FortiClient* Mac OS X	• 7.0.0 build 0022
FortiClient* Linux	• 7.0.0 build 0018
FortiClient* iOS	• 6.4.6 build 0507
FortiClient* Android	• 6.4.6 build 0539
FortiClient* EMS	• 7.0.0 build 0042
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 35
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiSandbox	• 2.3.3 and later, 4.0.0 is recommended

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS
13. FortiWLC
14. FortiNAC
15. FortiVoice
16. FortiDeceptor
17. FortiAI
18. FortiTester

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.1. When Security Fabric is enabled in FortiOS 7.0.1, all FortiGate devices must be running FortiOS 7.0.1.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *Get Checksum Code*.

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 and later need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

In the case when customers are using the following settings in 6.4:

```
config system settings
    set default-voip-alg-mode proxy-based
end

config firewall policy
    edit 0
        set inspection-mode flow
        unset voip-profile
    next
end
```

In 6.4, by default, SIP traffic is handled by proxy-based SIP ALG even though no VoIP profile is specified in a firewall policy.

After upgrading, the firewall policy will remain in `inspection-mode flow` but handled is by flow-based SIP inspection.

Due to the difference in which the SIP traffic is handled by flow-based SIP versus proxy-based SIP ALG inspection in 7.0.0 and later, if customers want to maintain the same behavior after upgrading, they can manually change the firewall policy's `inspection-mode` to `proxy`:

```
config firewall policy
    edit 0
        set inspection-mode proxy
        unset voip-profile
    next
end
```

Or prior to upgrading, they can assign a `voip-profile` to the firewall policies that are processing SIP traffic to force the conversion to `inspection-mode proxy` after upgrading.

L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later

If the setting is not manually updated after upgrading, the VPN connection will be established, but it will not be accessible from the internal network (office network). This setting change is necessary regardless of whether route-based or policy-based IPsec is used.

To make L2TP over IPsec work after upgrading:

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

```
config vpn l2tp
    set eip 210.0.0.254
    set sip 210.0.0.1
    set status enable
    set usrgrp "L2tpusergroup"
end
```

Add a static route after upgrading:

```
config router static
    edit 1
        set dst 210.0.0.0 255.255.255.0
        set device "l2t.root"
    next
end
```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1 and later, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`
- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects* > *NAT46 Policy*
- *Policy & Objects* > *NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects* > *Virtual IPs* related pages

During the upgrade process after the FortiGate reboots, the following message is displayed:

```
The config file may contain errors,
Please see details by the command 'diagnose debug config-error-log read'
```

The following output is displayed after running the diagnose command:

```
# diagnose debug config-error-log read
>>> "config" "firewall" "policy64" @ root:command parse error (error -
61)
>>> "config" "firewall" "policy46" @ root:command parse error (error -
61)
```

Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1 and later, you will need to manually create new `vip46` and `vip64` policies.

- Create a `vip46` from `config firewall vip` and enable the `nat46` option.
- Create a `vip64` from `config firewall vip6` and enable the `nat64` option.
- Create or modify `ippool` and `ippool6`, and enable the `nat64` or `nat46` option.
- Create a policy and enable the `nat46` option, apply the `vip46` and `ippool6` in a policy.
- Create a policy and enable the `nat64` option, apply the `vip64` and `ippool` in policy.
- Ensure the routing on the client and server matches the new `vip`/`vip6` and `ippool`/`ippool6`.

Example configurations

`vip46` object:

Old configuration	New configuration
`config firewall vip46` `edit "test-vip46-1"` `set extip 10.1.100.155` `set mappedip 2000:172:16:200::55` `next` `end`	`config firewall vip` `edit "test-vip46-1"` `set extip 10.1.100.150` `set nat44 disable` **`set nat46 enable`** `set extintf "port24"` **`set ipv6-mappedip 2000:172:16:200::55`** `next` `end`

`ippool6` object:

Old configuration	New configuration
`config firewall ippool6` `edit "test-ippool6-1"`	`config firewall ippool6` `edit "test-ippool6-1"`

Old configuration	New configuration
`set startip 2000:172:16:201::155` `set endip 2000:172:16:201::155` `next` `end`	`set startip 2000:172:16:201::155` `set endip 2000:172:16:201::155` **`set nat46 enable`** `next` `end`

NAT46 policy:

Old configuration	New configuration
`config firewall policy46` `edit 1` `set srcintf "port24"` `set dstintf "port17"` `set srcaddr "all"` `set dstaddr "test-vip46-1"` `set action accept` `set schedule "always"` `set service "ALL"` `set logtraffic enable` `set ippool enable` `set poolname "test-ippool6-1"` `next` `end`	`config firewall policy` `edit 2` `set srcintf "port24"` `set dstintf "port17"` `set action accept` **`set nat46 enable`** `set srcaddr "all"` `set dstaddr "test-vip46-1"` `set srcaddr6 "all"` `set dstaddr6 "all"` `set schedule "always"` `set service "ALL"` `set logtraffic all` `set ippool enable` `set poolname6 "test-ippool6-1"` `next` `end`

`vip64` object

Old configuration	New configuration
`config firewall vip64` `edit "test-vip64-1"` `set extip 2000:10:1:100::155` `set mappedip 172.16.200.155` `next` `end`	`config firewall vip6` `edit "test-vip64-1"` `set extip 2000:10:1:100::155` `set nat66 disable` **`set nat64 enable`** **`set ipv4-mappedip 172.16.200.155`** `next` `end`

`ippool` object

Old configuration	New configuration
`config firewall ippool` `edit "test-ippool4-1"` `set startip 172.16.201.155` `set endip 172.16.201.155`	`config firewall ippool` `edit "test-ippool4-1"` `set startip 172.16.201.155` `set endip 172.16.201.155`

Old configuration	New configuration
next end	set nat64 enable next end

NAT64 policy:

Old configuration	New configuration
config firewall policy64 edit 1 set srcintf "wan2" set dstintf "wan1" set srcaddr "all" set dstaddr "test-vip64-1" set action accept set schedule "always" set service "ALL" set ippool enable set poolname "test-ippool4-1" next end	config firewall policy edit 1 set srcintf "port24" set dstintf "port17" set action accept set nat64 enable set srcaddr "all" set dstaddr "all" set srcaddr6 "all" set dstaddr6 "test-vip64-1" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname "test-ippool4-1" next end

Product integration and support

The following table lists FortiOS 7.0.1 product integration and support information:

Web browsers	• Microsoft Edge 89 • Mozilla Firefox version 89 • Google Chrome version 91 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	• 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
FortiExtender	• 4.0.0 and later, 7.0.1 is recommended
AV Engine	• 6.00262
IPS Engine	• 7.00029

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESX	• Versions 4.0 and 4.1
VMware ESXi	• Versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 89 Google Chrome version 91
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 89 Google Chrome version 91
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 89 Google Chrome version 91
macOS Big Sur 11.3	Apple Safari version 14 Mozilla Firefox version 89 Google Chrome version 91
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 7.0.1. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
705591	When `av-scan` is enabled on the load end box, the FortiGate CPU hits 100% for over one minute. Such high CPU might cause WAD daemon signal 6 abort during that period.
706454	When AV and sandbox submission is enabled, `/tmp/cdr` is not cleaned after a scan when there are multiple concurrent sessions.
707186	Scanunit crashes with signal 11 when users attach files in the Outlook Web App.

Data Leak Prevention

Bug ID	Description
709845	DLP file pattern ID is still referenced by AV profile `analytics-wl-filetype` after FortiSandbox is disabled.

DNS Filter

Bug ID	Description
715317	Web filter service is not start properly when DNS filter is configured in a firewall profile group.

Endpoint Control

Bug ID	Description
666426	IPsec VPN does not have FCT client IP to send to EMS if using DHCP-over-IPsec.
685549	Need to check EMSC entitlement periodically inside fcnacd.

Bug ID	Description
707388	When EMS has an offline status, most of time the FortiClient de-registers from EMS and the client certificate will be empty in web browser certificate store.

Explicit Proxy

Bug ID	Description
638172	Proxy policy matching should support choosing the best internet service name when the IP matches multiple object names.
681054	Web proxy users are disconnected due to external resource update flushing the user even if they do not have an authentication rule using the related proxy address or IP list.
697566	Explicit proxy unable to access a particular URL (https://***.my.salesforce.com) after upgrading from 5.6.12 to 6.2.7.
700451	Wrong source IP used intermittently when FortiGate has SD-WAN and is transparently proxy forwarding to explicit proxy.
706078	Unable to access SSL exempt site with authentication TP proxy because certificate inspection does not learn the forward server object.
708851	When visiting a website for the first time in Firefox, the disclaimer page is shown and the webpage loads normally. When visiting a website for a second time, Firefox may take a few minutes to show the disclaimer and then another few minutes to load the webpage.
716224	In web proxy with transparent policy, the web filter rating fails when there is no SNI or CID.

Firewall

Bug ID	Description
591721	Viewing firewall shaping policy in the GUI will unset the `traffic-shaper` if `class-id` and `traffic-shaper` are both configured.
595949	Any changes to the security policy table causes the hit count to reset.
645010	Misleading GUI error when policy lookup fails due to source IP route lookup.
653137	VIP object associated with SD-WAN member interface from omni-select list of destination addresses should not be filtered out.
654356	In NGFW policy mode, sessions are not re-validated when security policies are changed.
681893	Firewall policy *Last Used* information is different in the CLI and GUI.

Bug ID	Description
688887	The CLI should give a warning message when changing the address type from `iprange` to `ipmask` and there is no subnet input.
694154	Dynamic traffic shapers are not consistent in their idle time limit.
696619	FGSP synchronized UDP sessions may be blocked in NGFW policy mode when asymmetric routing is used due to a policy matching failure. Other types of traffic may also be affected (such as TCP) in the case of failover of the reply direction traffic to a different FortiGate in the FGSP cluster.
705402	Server load-balancing on FortiGate is not working as expected when the active server is down.
707659	New ISBD object is not indicated in the GUI.
707854	FortiGate is not able to resolve FQDNs without DNS suffix for firewall address objects.
708159	Firewall policy is not applied correctly when using VNE tunnel interface with policy-based IPsec VPN.
709832	When there are multiple internet services configured that match a certain IP, port, or protocol, it may cause the wrong policy to be matched.
714198	When in transparent mode with AV and IPS, the original and reply direction traffic should be redirected only one time.
714647	Proxy-based policy with AV and web filter profile will cause VIP hairpin to work abnormally.
716317	IPS user quarantine ban event is marking the sessions as dirty.
717170	TCP MSS size for local traffic is not adjusted by the firewall policy.
717802	In transparent mode, a log has an irrelevant `policyid`.
718048	Some policy entries are lost when restoring a VDOM configuration if the `inspection-mode` is flow, and the `dstaddr` is the server load balance VIP.
719925	Load balancing is not allowed with a flow-based policy, even if the server type is configured as IP or TCP.
724145	Expiration timer of expectation session may show a negative number.

FortiView

Bug ID	Description
621453	FortiGate cannot get detailed information on FortiClient vulnerabilities from FortiAnalyzer.
683654	FortiView pages with FortiAnalyzer source incorrectly display a *Failed to retrieve data* error on all VDOM views when there is a newly created VDOM that is not yet registered to FortiAnalyzer. The error should only show on the new VDOM view.
701979	On the *Dashboard* > *FortiView Web Sites_FAZ* page, many websites have an *Unrated* category, and drilling down on these results displays no data.

Bug ID	Description
712580	When viewing FortiView *Sources* or *Destinations*, some usernames in the format of <DOMAIN\username> are displayed as *DOMAIN\username*. The user is displayed with a `\` in the CLI.
722543	The *Used Quota* cannot be sorted on the *FortiGuard Quota Monitor*. The *Used Quota* column has now been split into two sortable columns: *Used Traffic Quota* and *Used Time Quota*.

GUI

Bug ID	Description
585899	SAML auto configuration does not take `admin-sport` into account.
589231	When using the GUI to edit an IP/Wildcard Mask that was created using the CLI, the error message *Invalid IP/Wildcard mask.* is displayed.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches. This performance issue needs a fix on both FortiOS and FortiSwitch. A fix was provided in FortiOS 7.0.1 and FortiSwitch 7.0.1.
610572	Guest user credentials never expire if a guest user logs in via the WiFi portal while an administrator is actively viewing the user's account via the GUI. If the administrator clicks *OK* in the user edit dialog after the guest user has logged in, the user's current login session is not subject to the configured expiration time.
645158	When logging into the GUI via FortiAuthenticator with two-factor authentication, the FortiToken Mobile push notification is not sent until the user clicks *Login*.
647431	After removing an image name on the *Replacement Messages Edit* page, an image list should be displayed when hovering the mouse over the image URL link, but it is not.
665597	When `set server-identity-check` is enabled, *Test User Credentials* fails when performed on the CLI and passes when run from the GUI. The GUI implementation has been updated to match that of the CLI.
674548	When searching for a *Firewall Policy*, if the search keyword is found in the policy name and there are spaces adjacent to it, the search results will be displayed without the adjacent spaces. The actual policy name is not changed.
674592	When `config ha-mgmt-interfaces` is configured, the GUI incorrectly shows an error when setting overlapping IP address.
676104	Check mark for maximize bandwidth SD-WAN rule is not removed when member no longer meets SLA.
676306, 719694	When there is a connection issue between the FortiGate and a managed FortiSwitch, unexpected behavior might occur in httpsd when navigating between *Switch Controller* related GUI pages.
686592	GUI does not display statistical information on SD-WAN *Performance SLA* page.

Bug ID	Description
689392	Port *Errors* counters for managed FortiSwitches show a zero when the port is actually shows errors.
690666	Enabling daylight saving time (DST) results in GUI and CLI system time differences when DST is active (end of March to end of October).
691620	Use *Account Entitlement* when checking for FSAC contract.
695264	The save function does not work as expected for policies with certain applications selected.
695815	When editing the external connector *Poll Active Directory Server* from the GUI, the *Users/Groups* option is always an empty value, even if there is an existing group configured.
696226	Interfaces and zones open slowly.
696573	Firewall policy is not visible in GUI when using `set internet-service src enable`.
701442	Cannot access GUI for FortiGate in FIPS-CC mode.
701742	Items added to *Favorites* are lost after a logout or reboot.
702065	After upgrading to 6.4.4, the RADIUS server with non-FortiToken two-factor authentication does not work in the GUI.
703955	When editing the WAF profile in the GUI, changes to the WAF `default-allowed-methods` are not committed. The CLI must be used.
704209	When updating the *Disclaimer Page* replacement message, if the message is too long, the *Save* button is disabled and a red warning displays the current buffer size compared to the allowed size.
704503	Routing monitor is slow to load or does not load when the user has a full routing table.
704618	When login banner is enabled, and a user is forced to re-login to the GUI (due to password enforcement or VDOM enablement), users may see a *Bad gateway error* and HTTPSD crash.
706340	When editing a firewall policy, copying and pasting in the *Comments* field gives an error.
706711	When `accprofile` is set to `fwgrp custom` with all read-write permissions, some GUI menus will not be visible. Affected menu items include *IP Pools*, *Protocol Options*, *Traffic Shapers*, and *Traffic Shaping Policy/Profile*.
706982	Unable to edit interface address, get *Bits of the IP address will be truncated by the subnet mask* error.
708121	After a user creates or edits an SSID interface, the GUI incorrectly navigates to the interfaces list instead of SSIDs list.
708211	Administrators with VDOM scope cannot change their own password in the GUI.
708467	Cannot configure ZTNA to enable an IP or MAC filter type firewall policy to add ZTNA tag.
708947	Policy dialogs (*Firewall*, *NAT46*, *NAT64*, *Proxy*) sometimes get stuck loading due to an error when generating a security rating report.
709103	For certain configurations, editing interfaces from the GUI causes the httpsd process to spike in CPU usage.
709662	Static route for IPsec VPN shows tunnel ID as a gateway and provides an unreachable error.

Bug ID	Description
710220	Unable to download MIB files from FortiGate.
710946	Special characters not allowed in the OU field of a CSR signing request, from both the GUI and CLI.
713148	For certain configurations, various pages that have interface selects can cause high memory usage from httpsd and put the FortiGate into conserve mode.
713580	Non-FortiToken RADIUS two-factor authentication not working when logging into the GUI.
715256	When the *Security Fabric Connection* is enabled on a VPN interface, the *DHCP Server* section disappears from the GUI.
715493	For certain configurations, httpsd consumes high CPU when loading *Firewall* pages in a browser.
716986	GUI and REST API show incorrect reference count for web filter after adding and removing it from a policy.
717405	Tooltip for FortiSandbox Cloud shows status as *Unreachable or not authorized.*
719620	Interface page does not load for an administrator user with `netgrp read-write` permissions and an IPsec VPN is configured.
720006	GUI always shows duplicate entry when trying to create a NAC dynamic address and other types of firewall addresses.

HA

Bug ID	Description
659837	The HA secondary cannot synchronize a new virtual switch configuration from the primary.
670331	Management access not working in transparent mode cluster after upgrade.
678145	GUI shows a warning icon that the cluster is out of sync although the cluster is in sync.
692384	High memory usage of hasync process on FGCP passive device.
694646	ICMP session cannot synchronize after the FortiGate where the session was first created reboots.
697066	When SLBC HA has a fast flip, there is a chance that the route will be deleted from the secondary when it changes to the primary.
698732	Copied policy set to *Deny* contains unneeded lines.
703047	`hbdev` goes up and down quickly, then the cluster keeps changing rapidly. `hasync` objects might access invalid cluster information that causes it to crash.
703719	`hasync` is busy when receiving ARP when there is a huge number of ARPs in the network.
708928	The `set override disable` setting changes to enabled on main virtual cluster after rebooting (flag of second virtual cluster remains disabled).
709382	Creating an aggregate interface in HA causes the VMAC resolution to fail.

Bug ID	Description
710236	Heartbeat interfaces do not get updated under `diagnose sys ha dump-by <group | memory>` after HA `hbdev` configuration changes.
711521	When HA failover happens, there is a time difference between the old secondary becoming the new primary and the new primary's HA ID getting updated. If a session is created in between, the session gets a wrong HA ID, which indicates incorrectly that the session's traffic needs to be handled by the new secondary.
711962	Incorrect uptime value for HA secondary shown in the GUI.
714113	GRE configuration should not be synchronized in multi-AZ HA, but the system does not allow it to be added in the VDOM exception.
714404	Every UDP packet in the reply direction triggers the session state update synchronization, even if the session state did not change.
715939	Cluster is unstable when running interface configuration scripts. For example, when inserting many VLANs, hatalk will get a lot of `intf_vd_changed` events and recheck the MAC every time, which blocks hatalk from sending heartbeat packets for a long time so that the peer loses it.
716216	HA becomes out of sync when a backup device is updating the discarded duplicate BGP network table entry from the primary.
717251	In FGSP, `session-sync-dev` statistics of `get system ha status` disappear after reboot.
717525	FortiGate sends its serial number at the beginning of the file path via TFTP backup for CLI automation script or automation stitch when in the cluster.
717785	HA primary does not send anti-spam and outbreak prevention license information to the secondary.
721482	CLI help text should not list FortiManager as an option for `ha-direct`.
721720	Performance degradation of session synchronization after upgrading.
722284	When there is a large number of VLAN interfaces (around 600), the FortiGate reports `VLAN heartbeat lost on subinterface vlan` error for multiple VLANs.
740743	When enabling `lag-out-port-select`, both cluster units reboot simultaneously.

Intrusion Prevention

Bug ID	Description
680501	Destination interfaces are set to unknown for previous ADVPN shortcuts sessions.
682071	IPS signatures are not working with VIP in proxy mode.
686301	ipshelper CPU spikes when configuration changes are made.
689259	Flow-based AV scanning does not send specific extension files to FortiSandbox.
721462	Memory usage increases up to conserve mode after upgrading IPS engine to 5.00239.

IPsec VPN

Bug ID	Description
578879, 676728	IPsec tunnel bandwidth usage is not correct on the GUI widget and SNMP graph when NPU is doing host offloading.
620907	L2TP-over-IPsec tunnels frequently disconnect and hardly reconnect. CPU0 and CPU2 are at over 80%.
642760	Split tunnel is not working with L2TP IPsec VPN on Windows native VPN.
674576	Certificate-based IPsec authentication succeeds when the `strict-crl-check` is enabled and the CRL is not reachable.
691718	Traffic cannot pass through IPsec tunnel after FEC is enabled on server side if NAT is enabled between VPN peers.
708590	Framed IPv6 address is not used in IPsec or SSL VPN tunnels.
708870	After failover, the static tunnel interface's remote IP static routes are missing on the new primary.
708940	When ADVPN with BGP has `routing-protocol` and `link-down-failover` enabled, establishing the ADVPN shortcut establish causes the BGP neighbor to flap and affect traffic.
709850	Duplicate IP assigned by IKE Mode Config due to static gateway being out of sync after HA flapping. The tunnel that is out of sync cannot receive the deletion from the hub and holds on to an IP that has already been released.
710961	Hub is dropping packets due to `Failed to find IPsec Common` after upgrading from 6.2.6 to 6.2.7.
711072	ADVPN using BGP cannot bring up second shortcut after first shortcut is established with `net-device` enabled.
713763	IPsec aggregate is not sending outbound ESP traffic on FortiOS 7.0.
713839	In a redundant mode IPsec aggregate, the first aggregate member is always used to output traffic even if it is down.
714400	Dynamic IKEv2 IPsec VPN fails to establish after adding new phase 2 with mismatched traffic selector.
715070	OCVPN configuration change in one member reloads the BGP configuration of all the OCVPN members.
715651	iked crashed when clients from the same peer connect to two different dynamic server configurations that are using RADIUS authentication.
717082	FortiGate keeps initiating DHCP SA rekey after lifetime expires.
718617	In an IPsec tunnel XAuth with RADIUS, the RADIUS Accounting Stop packet is missing the Acct-Input-Octets/Acct-Output-Octets attribute.
719655	IPsec does not work in FG-VM after upgrading to 7.0.

Log & Report

Bug ID	Description
708890	Traffic log of ZTNA HTTPS proxy and TCP forwarding is missing policy name and FortiClient ID.
710344	Reliable syslog is sent in the wrong format when flushing the logs queued in the log daemon when working in TCP reliable mode.
711946	FortiAnalyzer cannot process the packet loss field in the log because the field has a `%` in it.
712037	FortiAnalyzer OFTP connection is re-initialized every 30 seconds when the FortiGate connects to an unauthorized FortiAnalyzer.
722315	System might generate garbage administrator log events upon session timeout.
726231	The default `logtraffic` setting (UTM) in a security policy unexpectedly generates a traffic log.

Proxy

Bug ID	Description
670339	Proxy-based SSL out-band-probe session has local out connection. Since the local out session will not learn the router policy, it makes all outbound connections fail if there is no static router to the destination.
676419	WAD crash at `wad_async_queue` in FOH connect case.
683844	In cases when WAD fails to resolve a firewall policy for the session, WAD crashes at `wad_ssl_proxy_can_bypass()` when a missed condition check allows the session to still pass through.
700073, 714109	YouTube server added new URLs (`youtubei/v1/player, youtubei/v1/navigator`) that caused proxy option to restrict YouTube access to not work.
700481	Unable to authenticate to FTP server when firewall policy is set to proxy-based and AV is enabled.
701513	WAD encounters segmentation fault crash at `wad_http_scan_engine__on_unblock`.
704323	In IPS TCP proxy handover, the firewall policy `tcp-mss-sender`, `tcp-mss-receiver`, and interface `tcp-mss` settings are not used.
706555	WAD crashes at `wad_ssl_port_p2s_set_server_cert`.
706556	WAD crashes at `wad_http_scan_safe_proc_msg`.
708514	WAD crash at `flush sec_profile` after deleting VDOM.
709391	Enhance link monitor health check for access proxy real server in ZTNA.
709623	WAD crashes seen in user information upon user purge and during signal handling of user information history.
710125	All load-balancing methods should be supported for ZTNA access proxy.

Bug ID	Description
710737	For firewall policies with `http-policy-redirect` enabled and `ssl-ssh-profile` is set to `inspect-all certificate-inspection`, WAD is unable to block the traffic when proxy policy matching fails.
711484	Certificate authentication support should be added to the normal proxy policy authentication.
714610	Explicit proxy policy (ISDB and IP pool) cannot be set in the GUI or CLI.
715327	The `cert-probe-failure` option is not available when `inspect-all certificate-inspection` is enabled.
716400	Certificate inspection is not working as expected when an external proxy is used.
719681	Flow control failure occurred while transferring large files when `stream-scan` was running, which sometimes resulted in WAD memory spike.
724445	Local TCP/853 unexpectedly open as soon any proxy mode inspection policy with UTM is enabled.
724968	Certificate inspection profile is doing a deep scan for an FTPS SSL exchange.
726801	When FortiGuard is updating, an external resource build might happen at the same time with other RAM consuming update operations, causing the system to enter conserve mode.
728078	Rating request does not always check cache.

REST API

Bug ID	Description
597494	REST API incorrectly returns error code 401 (authentication error) instead of 403 (authorization error) for requests that pass the authentication check but are not permitted to access the resource.
710198	`/api/v2/monitor/system/available-interfaces` takes over one minute for a response.
713445	For API user tokens with CORS enabled and set to wildcard *, direct API requests using this token are not processed properly. This issue impacts FortiOS version 5.6.1 and later.
714075	When CORS is enabled for REST API administrators, POST and PUT requests with body data do not work with CORS due to the pre-flight requests being handled incorrectly. This only impacts newer browser versions that use pre-flight requests.

Routing

Bug ID	Description
579884	VRF configuration in WWAN interface has no effect after reboot.

Bug ID	Description
670031	LDAP traffic that originates from the FortiGate is not following SD-WAN rule.
682455	Checkmark is not shown beside the interface currently selected by the SD-WAN rules (*Network > SD-WAN Rules* page).
688317	Blackhole route to the gateway of policy route makes the PBR inactive/disabled.
697645	FortiGate deletes `prefix-list` configuration due to concurrent administrator SSH sessions.
699122	Issues with SD-WAN zone's availability to select it as an OSPF interface.
700840	VRF should support for IPv6 in static route and BGP VRF leaking table.
701027	No speed test button for PPPoE interface in GUI on *Interfaces* page.
702463	Security rating traffic does not follow SD-WAN rules.
703782	Traffic to FortiToken Mobile push server does not follow SD-WAN/PBR rules.
705767	SD-WAN rules are not working with route tags and VRF.
706237	ICMP *Destination Host Unreachable* responses are sent in reverse order.
707143	Suggest adding an option for NetFlow to use SD-WAN.
707713	Restore the change of routing code.
708614	Firewall policy rule with destination interface as `virtual-wan-link` cannot match traffic in some cases.
710606	Some static routes disappear from RIB/FIB after modifying or installing static routes by running a script in the GUI.
712586	SNAT sessions on the original preferred SD-WAN member will be flushed after the preferred SD-WAN member changes, so existing SNAT traffic will be interrupted.
715274	Enabling SD-WAN on interfaces with full BGP routes leads to device going into conserve mode.
718950	Local out routing does not work with PPPoE interface.
719788	*Policy Routes* GUI page does not show red exclamation mark when a source or destination is negated, like on *Firewall Policy* page.
722343	SD-WAN rule not matched with MAC address object and ISDB in policy.
723550	Load-balance service mode and maximize bandwidth (SLA) in SD-WAN rule does not work as expected in 7.0.0.
723726	TCP session drops between virtual wire pair with `auto-asic-offload` enabled in policy.
724250	Enabling `preserve-session-route` does not take effect in SD-WAN scenario.
724887	`set interface-select-method` takes a long time to take effect for DNS local out traffic when the source IP is specified.
727812	ADVPN does not work with RIP as the routing protocol when `net-device` is enabled.

Security Fabric

Bug ID	Description
685642	Link to *Login toFortiAnalyzer* on *Physical Topology* page does not open, and FortiAnalyzer HTTPS is no longer configured on port 443.
695040	Unable to connect to vCenter using ESXi SDN connector with password containing certain characters.
708172	Automation stitch action does not work when trigger is an AV and IPS database update.
712155	The security rating for *Admin Idle Timeout* incorrectly fails for a FortiAnalyzer with less than 10 minutes.
714807	Security rating two-factor authentication test shows as failed for IPsec and SSL VPN, but all users have two-factor authentication enabled.
716698	Multiple ACI Direct connectors are not supported.
718469	Wrong timestamp printed in the event log received in email from event triggered from email alert automation stitch.
718581	If HA management interface is configured, the Kubernetes connector fails to connect.
719029	Automation stitch action no longer understands `%%log.date%%` and `%%log.time%%` variables.
722950	Topology page is empty in robot Security Fabric setup.

SSL VPN

Bug ID	Description
500664	SSL VPN RDP bookmark not working with CVE-2018-0886.
515519	guacd uses 99% CPU when SSL VPN web portal connects to RDP server.
542815	SSL VPN web portal RDP connections to RDS session hosts fails.
550819	guacd is consuming too much memory and CPU resources during operation.
586035	The policy `script-src 'self'` will block the SSL VPN proxy URL.
630068	When SSL VPN SSH times out, SSH to SES will crash when SSH is empty.
659581	Google Maps and 2gis.ru page do not display the map at all in SSL VPN web portal.
669707	The jstor.org webpage is not loading via SSL VPN bookmark.
671647	Imported certificate cannot be used in IPsec tunnel only (*-3: Entry not found*).
676333	Unable to type accents using dead keys in RDP using Spanish keyboard layout over SSL VPN web mode in macOS.

Bug ID	Description
677031	SSL VPN web mode does not rewrite playback URLs on the internal FileMaker WebDirect portal.
677057	SSL VPN firewall policy creation via CLI does not require setting user identity.
677548	In SSL VPN web mode, options pages are not shown after clicking the option tag on the left side of the webpage on an OWA server.
677668	sslvpnd crashes due to wrong application index referencing the wrong shared memory when daemons are busy. Crash found when RADIUS user uses Framed-IP.
678757	vCenter (*.be***.tld) page does not load in SSL VPN web mode.
689465	RDS redirect not working on SSL VPN web portal.
693200	Error when logging out SSL VPN bookmark website.
693237	DCE/RPC sessions are randomly dropped (`no session matched`).
693347	Forward traffic for SSL VPN with EMS tags dynamic address is failing apart from helper-based traffic.
693519	SSL VPN authentication fails for PKI user with LDAP.
693718	FortiClient SSL VPN users are unable to authenticate when zero-trust tag IP address is used as the host IP under limited access.
694226	SSL VPN web mode removes ant-tree components in HTML source.
694346	Report section of internal web server (https://lm***.lm***.au***.vw***/ar***/) is not accessible via the SSL VPN web portal.
694671	PDF files on internal web server, https://co***.ag***.em***.vw***:8443, are not opening in SSL VPN web portal.
695404	WALLIX personal bookmark issue in SSL VPN portal.
695457	JS error thrown when accessing HTTPS bookmark (mk***.ag***.cp***.vw***) via SSL VPN web portal.
695763	FortiClient iOS 6.4.5 has new feature that allows bypassing of 2FA for SSL VPN 2FA. The FortiGate should allow access when 2FA is skipped on FortiClient.
696533	Certain URLs are not rewritten for bookmarked HTTPS external site http://www.sz***.hu.
697551	Unable to save record on internal website https://1**.1**.8*.3*/Login.jsp via SSL VPN web mode.
701119	SSL VPN DTLS tunnel could not be established in some cases when the tunnel link is still under negotiation. Some IP packets were sent to the client, causing the client's logic to fail.
704597	Search option on internal website, kp***.kd****.ca, not working while accessing via SSL VPN web mode.
705278	DTLS SSL VPN connection cannot be established via FortiTester.
705370	Back-end server (va***.ra***.com.ar) is not working in SSL VPN web mode.
706185	OWA user details are not showing in SSL VPN web mode.

Bug ID	Description
707792	SSL VPN connection breaks when deleting irrelevant CA and PKI is involved.
708021	SSO authentication to FortiMail webmail is not working using SSL VPN bookmark.
708639	Idle timeout does not send log out request to IdP for SAML login on SSL VPN portal.
710163	SSL VPN stuck loading https://el***.***-data.pl when wrong credential was entered.
711503	SSL VPN web mode access to internal web server http://10.2.1.78 is broken after upgrading to 7.0.0.
711690	QNAP NAS web page hangs on loading page after entering the credentials in SSL VPN web mode.
711944	POP3 authentication failed for SSL VPN.
712880	Windows Admin Center webpage (ge***.ov***) does not load correctly in SSL VPN web mode.
714604	SSL VPN daemon may crash when connection releases.
714700	SSL VPN proxy error in web mode due to requests to loopback IP.
715928	SSL VPN signal 11 crashes at `sslvpn_ppp_associate_fd_to_ipaddr`. For RADIUS users with Framed-IP using tunnel mode, the first user logs in successfully, then a second user with the same user name logs in and kicks the first user out. SSL VPN starts a five-second timer to wait for the first user resource to clean up. However, before the timer times out, the PPP tunnel setup fails and the PPP context is released. When the five-second timer times out, SSL VPN still tries to use the PPP context that has already been released and causes the crash.
716622	Due to change on samld side that increases the length of the SAML attribute name to 256, SSL VPN could not correctly parse the username from the SAML response when the username attribute has a long name.
717193	Website cannot be accessed in SSL VPN web mode.
717382	Website, co***.gob.pe, is not shown properly in SSL VPN web mode.
718142	The map integrated in the public site is not visible when using SSL VPN web mode.
718159	Webpage, http://10.3.24.8/ma***, is not displaying correctly in SSL VPN web mode.
718170	SSL VPN web portal does not show thumbnails of videos for an internal JS-based web server.
718262	Traffic cannot go through SSL VPN tunnel when a second user kicks first session off.
719069	iprope records for SSL VPN policies are removed after upgrading to 7.0.0 or during the reboot.
720290	Internal webpage, https://172.3**.***.164/ce***/, is not loading in SSL VPN web mode.
721427	Unable to load NetApp OnCommand Unified Manager webpages due to reloading loop in SSL VPN web mode.
723498	Sometimes in tunnel mode with a lot of tunnels, the file descriptor to the `mux dev` is not closed, which causes the memory to linger until the process is killed.
724830	FortiGate sends authentication request to all RADIUS servers instead of only those in the default realm.

Bug ID	Description
726576	Internal webpage with JavaScript is not loading in SSL VPN web mode.
726641	Unable to load pi***.vi***-ga***.org in SSL VPN web mode.

Switch Controller

Bug ID	Description
647817	Configuration changes on the FortiGate not taking effect on the FortiSwitch.
682430	Entry created in NTP under interface configuration after failing to enable FortiLink interface.
699533	In FortiOS 7.0.0, the default authentication protocol for a switch controller SNMP user is SHA256, as opposed to the default SHA1 in previous versions.
702942	FortiLink trunk is not formed on FortiSwitch connecting to FortiGate. When managed switches are learned on the software switch and hardware switch, they were deleted from the CLI, and `fortilinkd` did not clear the states for those switches so new switches were not learned.
717506	Unable to add description on shared FortiSwitch port.

System

Bug ID	Description
464382	TFTP client always tries binding to port 1069, which is a part of dynamic port range. Other daemons sometimes use this port, which results in a TFTP bind failure.
568399	FG-200E has `np6lite_lacp_lifc` error message when booting up a device if there are more than seven groups of LAGs configured.
572038	VPN throughput dropped when FEC is enabled.
613947	Redundant interface cannot pick up traffic if one member is down.
627734	Optimize interface dialog and configuration view for `/api/v2/monitor/system/available-interfaces` (phase 1).
651626	A session clash is caused by the same NAT port. It happens when many sessions are created at the same time and they get the same NAT port due to the wrong port seed value.
664856	A VWP named .. can be created in the GUI, but it cannot be edited or deleted.
666418	SFP interfaces on FG-330xE do not show link light.
667307	Console prints out `NP6XLITE: np6xlite_hw_ipl_rw_mem_channel timeout` message on SoC4 platforms.
671332	httpsd crashed after changing VDOM for interface.

Bug ID	Description
674616	VDOM list is slow to load in GUI when there are many VDOMs configured on FG-3000D.
683387, 711698	Change WWAN interface default netmask to /32 and default distance to 1.
686903	DHCP option 121 as a client not working on FortiGate.
687833	Add DNS server selection method to change how DNS servers are configured and prioritized.
688009	Update built-in modem firmware that comes with the device in order for the SIM to be correctly identified and make LTE link work properly.
689317, 698927	After pushing the interface configuration from FortiManager, the device index is incorrectly set to 0.
690797	Huawei E8372h-320 LTE modem does not receive IP on FG-30E.
693757	Secondary FG-5001D blades in SLBC cluster do not show updated contract dates.
696550	Mirroring of decrypted SSL traffic does not work in flow mode; if the receiving side is a VM machine, the receiver is unable to receive SSL decrypted packets.
696556	Support `gtp-enhance-mode` (GTP-U) on FG-3815D.
696622	FortiGate cannot get gateway from built-in LTE modem on all LTE capable FortiGate platforms.
697287	FOS 6.2.6 in FIPS mode with LB VIP and custom ciphers does not allow traffic through.
698005	In some environments, host-side DPDK affects the benchmark result.
699358	Cannot change FEC (forward error correction) on port group 13-16.
699902	SNMP query of fgFwPolTables (1.3.6.1.4.1.123456.101.5.1.2.1) causes high CPU on a specific configuration.
700272	ddnsd did not update the new IP address of dynupdate.no-ip.com, so it failed to connect to the DDNS server.
700314	ARP reply sent out by FortiGate but was not received on neighbor device.
701839	CLI console shows `poll loop hangs` error messages after booting up the device.
701911	FortiGate entered conserve mode (`service=kernel`), possibly due to large number of log creation requests.
702135	cmdbsvr memory leak due to unreleased memory allocated by OpenSSL.
703872	Unable to change speed and status of hardware switch member on SoC3 and SoC4 platforms with virtual switch feature.
704981	LLDP transmission fails if there are nested software switches.
705878	Local certificates could not be saved properly, which caused issues such as not being able to properly restore them with configuration files and causing certificates and keys to be mismatched.
706131	When processing visibility log requests and passively learning FQDNs and wildcard FQDN addresses at a high rate, the CPU usage of dnsproxy can reach 90% or higher.

Bug ID	Description
709513	SD-WAN reports phantom packet loss.
710807	FGR-60F WAN1 and WAN2 fail to connect to the network due to board ID GPIO assignment being incorrect.
710934	FortiGate loses its DHCP lease, which is caused by the DHCP client interface turning into initial state (from that point dhcpcd will send out discover packets), but old IPs and router are still in the kernel, so it can reply to the ICMP request. That causes the customer's DHCP server (a router) to fail to assign the only available IP in the pool.
712203	Memory leak happens in forticron process, if GUI REST API caching is enabled.
712321	Multiple ports flapping when a single interface is manually brought up. Affected platforms: FG-3810D and FG-3815D.
712506	25G-capable ports do not receive any traffic. Affected platforms: FG-1100E and FG-1101E.
712905	Daylight saving time changes will not reflect for time zone 16.
713324	Command fail when running `execute private-encryption-key <xxx>`.
714164	SNMP times out or has slow response when SNMP queries FortiGate session table OIDs.
714192	`diagnose sys bcm_intf cli "2:"` and `diagnose sys bcm_intf cli "ps"` try to access a non-existent BCM switches, which leads to kernel panic.
714256	A softirq happened in an unprotected session read lock and caused a self-deadlock.
714402	FortiGate crashes after reboot (`kernel BUG at drivers/net/macvlan.c:869`).
714711	NP offloading is blocking backup traffic.
714805	FortiManager shows auto update for down port from FortiGate, but FortiGate event logs do not show any down port events when user shuts down the `ha monitor dev`.
715043	*Guest Management* page *Expire* column shows incorrect value for guest groups when set to expire after on first login.
715048	When there is no PRP setting in the 6.4 configuration, after upgrading from 6.4 to 7.0, kernel panic happens after enabling PRP.
715234	Packets are dropped for 30 seconds during or after massive configuration commit.
715571	`config match` command is not available in the user group configuration within the root VDOM when split-task VDOM is used.
716483	DNS proxy is case sensitive when resolving FQDN, which may cause DNS failure in cases where local DNS forwarder is configured.
717203	When user changes a configurations in the CLI, cmdbsvr sends the auto update file to FortiManager at the same time. There is a timing issue that may cause the last command not be sent to FortiManager since cmdbsvr has finished sending it, but the last command is not yet stored in the auto update file.
717791	`execute restore vmlicense tftp` fails with `tftp: bind: Address already in use`.

Bug ID	Description
718322	FortiGate sends an invalid configuration to FortiManager, which causes the FortiManager policy packages to have an unknown status.
718501	Problem resolving DNS TXT type queries with FortiGate.
718571	In cases where there are a lot of DHCP relay interfaces (such as 1000) and an interface is added or deleted, DHCP relay takes a long time to release and initialize all interfaces before it works again.
721119	The forticron process uses high CPU.
721733	IPv6 networks are not reachable shortly after FortiGate failover because an unsolicited neighbor advertisement is sent without a router flag.
721789	Account profile settings changed after firmware upgrade.
722287	The `set key-outbound` and `set key-inbound` parameters are missing for GRE tunnels under `config system gre-tunnel`.
723491	When ACME service is enabled on an interface, HTTPD responds to HTTP TRACE method with `HTTP 200 OK`.
723643	FortiGate NTP server cannot synchronize time for Linux client on IPv6.
725934	Running `execute tac report` or `diagnose debug report` via SSH leaves a tac_report* file in /tmp.

Upgrade

Bug ID	Description
701571	After upgrading from 6.4.5 to 7.0.0, all flow-based polices are switched to proxy if there is a SIP profile attached to the firewall policy.
708250	Console prints `__set_clr_flag:wwan ioctl failed, flag:0x0200 errno:19` when upgrading from 6.4.5 to 7.0.0.
710465	Policy inspection mode gets changed to proxy after upgrading to 7.0.0.
713724	SD-WAN health check over IPsec interfaces no longer work if there is a specified gateway under the IPsec SD-WAN member.
713878	Under `config system dns-database`, the `set type slave` configuration in 6.4.5 does not change to `set type secondary` after upgrading to 7.0.0.
716912	SSH access may be lost in some cases after upgrading to 6.2.8, 6.4.6, or 7.0.0.

User & Authentication

Bug ID	Description
688989	Two-factor authentication can be bypassed with some configurations.
697278	SAML entity ID can only be entered in HTTP format, but as per standard should also support URN.
698602	LDAP query from GUI does work in non-management and non-root VDOM.
698716	RADIUS password encoding does not work.
700838	FortiOS does not prompt for token when using RADIUS and two-factor authentication to connect to IPsec IKEv2.
704708	Local CA certificate, Fortinet_CA_SSL, cannot be restored from saved configuration file after the FortiGate factory reset.
707578	If a certificate authentication job expires in fnbamd, an error is returned to caller that makes the proxy block client traffic.
707868	The authd daemon crashes due to invalid dynamic memory access when data size is over 64K.
710212	RADIUS accounting port is occasionally missing.
712354	Firewall policy does not allow multiple SAML users that reference the same SAML server.

VM

Bug ID	Description
685782	HTTPS administrative interface responds over heartbeat port on Azure FortiGate despite `allowaccess` settings.
703457	Password reset via Azure portal does not work in cases where the DependencyAgentLinux extension is installed.
708768	On FG-VM-AWS, secondary IPs are missing after failover event.
710941	FortiOS GUI shows *Unable to connect to FortiGuard servers* warning when offline license is being used.
713279	After rebooting a GCP FortiGate, it takes more than 30 to 40 minutes to come up and affects passthrough traffic during this period.
714682	GENEVE tunnel with loopback interface is not working.
715750	EIP information is not automatically updated after instance reboot.
716161	Azure HA failover encounters error when doing route failover.
722227	If GCP SDN connector is using batch API call to collect dynamic addresses and any of the individual API calls in a batch all failed, cmdbsvr daemon CPU usage will be high, which may cause the GUI to get stuck and be unable to make configuration changes.

VoIP

Bug ID	Description
682983	SIP ALG does not DNAT all IP addresses in the SIP response messages (route field).

WAN Optimization

Bug ID	Description
702876	FortiGate web cache does not work in proxy mode.

Web Filter

Bug ID	Description
593203	Cannot enter a name for the web rating override or save it due to name input error.
717619	Running a remote CLI script from FortiManager can create a duplicated FortiGuard web filter category.
723610	Antiphishing LDAP domain verification is not matching credentials.

WiFi Controller

Bug ID	Description
502080	`TARGET ASSERT` error in WiFi driver causes kernel panic.
529727	The configured MAC address of the VAP interface did not take effect after rebooting.
662615	FG-80F series should support a total of 96 WTP entries (48 normal).
645328	Operating channel is 0 for both of the FAP radios (FAP-421E).
676689	RADIUS traffic not matching SD-WAN rule when using wpad daemon for wireless connection.
685593	Spectrum analysis graphs only presents a portion of the data for monitor mode radio when *X-Axis* is *MHz*.
693217	`Physical AP leave` log messages showing `reason="N/A"`.
693973	Captive portal/disclaimer is not shown for SSIDs not belonging to the default VRF.

Bug ID	Description
697058	Unable to change AP state under rogue AP's monitor page.
698961	FWF-60F/61F and FWF-40F encounters kernel panic (`LR is at capwap_find_sta_by_mac`) when one managed FortiAP is authenticating WiFi clients.
699905	FAP-421E does not come online over IPsec tunnel and shows a certificate error.
703685	VLAN-tagged CAPWAP traffic was dropped by NP6XLite FortiGate when FortiAP is connected through aggregate FortiLink FortiSwitch.
708449	CAPWAP traffic without VLAN tag was dropped by NP6XLite FortiGate when FortiAP is connected through an aggregate interface (no FortiLink).
709824	Dynamic VLAN SSID traffic cannot pass through VDOM link when `capwap-offload` is enabled.
709871	After the firmware upgrade, the AP cannot register to the central WLC because NPU offload changed the source and destination ports from 4500 to 0.
710759	Automation trigger for rogue AP on wire sends email alerts for rogue AP not on wire.
717227	`get wireless-controller wtp-status` output only shows only one AP entry.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
669673	FortiOS 7.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2022-26103
686912	FortiOS 7.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2021-32600
689909	FortiOS 7.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2022-22306
710161	FortiOS 7.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2021-24018
712334	FortiOS 7.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2021-26110
726300	FortiOS 7.0.1 is no longer vulnerable to the following CVE Reference: • CVE-2021-36169

Known issues

The following issues have been identified in version 7.0.1. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Endpoint Control

Bug ID	Description
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. **Workaround**: delete the EMS Cloud entry then add it back.

Firewall

Bug ID	Description
727790	The `diagnose internet-service info` command should show multiple matching entries for the same IP, port, or protocol.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.
699508	When an administrator ends a session by closing the browser, the administrator timeout event is not logged until the next time the administrator logs in.

Bug ID	Description
707589	*System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. **Workaround**: use Chrome, Edge, or Safari as the browser.
713529	When a FortiGate is managed by FortiManager with FortiWLM configured, the HTTPS daemon may crash while processing some FortiWLM API requests. There is no apparent impact on the GUI operation.
720657	Unable to reuse link local or multicast IPv6 addresses for multiple interfaces from the GUI. **Workaround**: use the CLI.
722832	When LDAP server settings involve FQDN, LDAPS, and an enabled server identity check, the following LDAP related GUI items do not work: LDAP setting dialog, LDAP credentials test, and LDAP browser.
734417	GUI incorrectly displays a warning saying there is not a valid upgrade path when upgrading firmware from 7.0.0 or 7.0.1 to 7.0.1 or 7.0.2.
735248	On a mobile phone, the WiFi captive portal may take longer to load when the default firewall authentication login template is used and the user authentication type is set to HTTP. **Workaround**: edit the login template to disable HTTP authentication or remove the href link to googleapis.
738027	The *Device Inventory* widget shows *no results* when there are two *user_info* parameters. **Workaround**: use the CLI to retrieve the device list.
743477	On the *Log & Report* > *Forward Traffic* page, filtering by the *Source* or *Destination* column with negation on the IP range does not work.
745325	When creating a new (public or private) SDN connector, users are unable to specify an *Update interval* that contains *60*, as it will automatically switch to *Use Default*.
745998	An IPsec phase 1 interface with a name that contains a / cannot be deleted from the GUI. The CLI must be used.
746953	On the *Network* > *Interfaces* page, users cannot modify the TFTP server setting. A warning with the message *This option may not function correctly. It is already configured using the CLI attribute: tftp-server.* appears beside the *DHCP Options* entry. **Workaround**: use the CLI.

HA

Bug ID	Description
701367	In an HA environment with multiple virtual clusters, *System* > *HA* will display statistics for *Uptime*, *Sessions*, and *Throughput* under virtual cluster 1. These statistics are for the entire device. Statistics are not displayed for any other virtual clusters.

IPsec VPN

Bug ID	Description
729879	Static IPsec tunnel with signature authentication method cannot be established on FIPS-CC mode FortiGate because the certificate subject verification changes to RDN bitwise comparison based.
730449	SD-WAN service traffic will be interrupted after upgrading to 7.0.1 if all of the following conditions are matched in its 6.4.x configuration: • Using `set gateway enable` in a particular SD-WAN service • Having `mode-cfg` configured • Not having ADVPN configured on the hub **Workaround**: Before upgrading, update the hub and spoke configurations as follows: • On the hub, enable the `exchange-interface-ip` option on the dial-up phase1 interface with `mode-cfg` configured. • On the spoke, enable `auto-discovery-receiver` on the related phase1 interface.
740624	FortiOS 7.0 has new design for dialup VPN (no more route tree in the IPsec tunnel), so traffic might not traverse over the dialup IPsec VPN after upgrading from FortiOS 6.4.6 to 7.0.1, 7.0.2, or 7.0.3 if the server replies on the static route over the dynamic tunnel interface to route the traffic back to the client. **Workaround**: configure the `src-subnet` on the client phase 2 interface. Then, static routes will be added by IKE on the server side (`add-route enable` is required). `config vpn ipsec phase2-interface` `edit <name>` `set src-subnet <x.x.x.x/x>` `next` `end`
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.

Proxy

Bug ID	Description
724670	Crash seen in WAD user information daemon when updating user group count upon user log off.
727629	An error case occurs in WAD while handling the HTTP requests for an explicit proxy policy.
735893	After the Chrome 92 update, in FOS 6.2, 6.4, or 7.0 running an IPS engine older than version 5.00246, 6.00099, or 7.00034, users are unable to reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.

REST API

Bug ID	Description
731136	The following API has a change in response format, which may break backward compatibility for existing integration: `POST /api/v2/monitor/system/config/restore` New format results: `{'config_restored': True}` Old format results: `{'restore_started': True, 'session_id': 'nTuRkV'}` Note that only the response format is changed. The actual configuration restoration operation still works as before. The integration application should handle this new response format so it can return correct response message back to the user.

Routing

Bug ID	Description
745856	The default SD-WAN route for the LTE wwan interface is not created. **Workaround**: add a random gateway to the wwan member. `config system sdwan` `  config members` `  edit 2` `  set interface "wwan"` `  set gateway 10.198.58.58` `  set priority 100` `  next` `  end` `end`

Security Fabric

Bug ID	Description
726831	Security rating for *Local Log Disk Not Full* reporting as failed for FortiGate models without log disks.
731292	Dashboard *Security Fabric* widget takes a long time to load in the GUI.
733511	Automation stitch trigger count does not update when target device is a downstream device.

SSL VPN

Bug ID	Description
718133	In some conditions, the web mode JavaScript parser will encounter an infinite loop that will cause SSL VPN crashes.
757450	SNAT is not working in SSL VPN web mode when accessing an SFTP server.

Switch Controller

Bug ID	Description
723501	When STP is enabled on a hardware switch interface, FortiLink loses its connection to FortiSwitch.

System

Bug ID	Description
644782	A large number of detected devices causes httpsd to consume resources, and causes entry-level devices to enter conserve mode.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
708228	A DNS proxy crash occurs during `ssl_ctx_free`.
715978	NTurbo does not work with EMAC VLAN interface.
728647	DHCP discovery dropped on virtual wire pair when UTM is enabled.
751715	Random LTE modem disconnections due to certain carriers getting unstable due to WWAN modem USB speed under super-speed.
756713	Packet loss on the LAG interface (eight ports) using SFP+/SFP28 ports in both static and active mode. Affected models: FG-110xE, FG-220xE, and FG-330xE.

User & Authentication

Bug ID	Description
750551	DST_Root_CA_X3 certificate is expired. **Workaround**: see the Fortinet PSIRT blog, https://www.fortinet.com/blog/psirt-blogs/fortinet-and-expiring-lets-encrypt-certificates, for more information.
754725	After updating the FSSO DC agent to version 5.0.0301, the DC agent keeps crashing on Windows 2012 R2 and 2016, which causes lsass.exe to reboot.
778521	SCEP fails to renew if the local certificate name length is between 31 and 35 characters.

VM

Bug ID	Description
729811	ASG synchronization is lost between secondary and primary instances if the secondary instance reboots. Affected platforms: all public cloud VMs and KVMs. **Workaround**: run `execute factoryreset2` on the secondary instance, and reconfigure the auto scaling group.

Built-in AV Engine

Resolved engine issues

Bug ID	Description
646129	Scanuit crash with signal 14 causing issues with POP3 traffic.
671820	Scanunit crashes in AV engine at `load_SearchFile;` trace leads to CDR PDF decoder.
691412	Scanunit process crashes when user accesses a specific website.
696525	Scaunit crash in AV engine in CDR code, signal 11.
706454	When AV and sandbox submission is enabled, `/tmp/cdr` is not cleaned after a scan when there are multiple concurrent sessions.

Built-in IPS Engine

IPS Engine 7.00029 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com