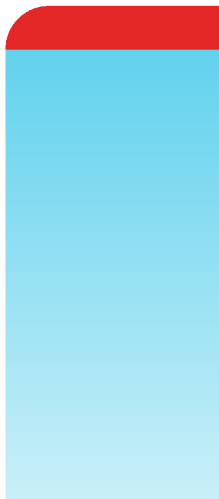


Release Notes

FortiOS 7.0.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



July 16, 2021

FortiOS 7.0.1 Release Notes

01-701-721490-20210716

TABLE OF CONTENTS

Change Log	6
Introduction and supported models	7
Supported models	7
Special notices	8
Azure-On-Demand image	8
GCP-On-Demand image	8
ALI-On-Demand image	8
SSL traffic over TLS 1.0 will not be checked and will be bypassed by default	9
Part numbers of unsupported FG-10xF, FGR-60F, and FGR-60F-3G4G Generation 2 models	9
L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1	9
Add interface for NAT46 and NAT64 to simplify policy and routing configurations	10
Upgrading	10
Creating new policies	10
Example configurations	11
Changes in CLI	13
Changes in GUI behavior	14
Changes in default behavior	15
Changes in table size	16
New features or enhancements	17
Upgrade information	24
Fortinet Security Fabric upgrade	24
Downgrading to previous firmware versions	25
Firmware image checksums	26
IPsec interface MTU value	26
HA role wording changes	26
Strong cryptographic cipher requirements for FortiAP	26
How VoIP profile settings determine the firewall policy inspection mode	27
Product integration and support	28
Virtualization environments	28
Language support	29
SSL VPN support	30
SSL VPN web mode	30
Resolved issues	31
Anti Virus	31
Data Leak Prevention	31
DNS Filter	31
Endpoint Control	31
Explicit Proxy	32

Firewall	32
FortiView	33
GUI	34
HA	36
Intrusion Prevention	37
IPsec VPN	37
Log & Report	38
Proxy	38
REST API	39
Routing	40
Security Fabric	41
SSL VPN	41
Switch Controller	44
System	44
Upgrade	47
User & Authentication	48
VM	48
VoIP	49
WAN Optimization	49
Web Filter	49
WiFi Controller	49
Common Vulnerabilities and Exposures	50
Known issues	51
Application Control	51
Endpoint Control	51
Firewall	51
GUI	51
HA	52
Intrusion Prevention	52
IPsec VPN	53
Proxy	53
REST API	53
Security Fabric	54
Switch Controller	54
System	54
User & Authentication	55
VM	55
WAN Optimization	55
WiFi Controller	55
Built-in AV engine	56
Resolved engine issues	56
Built-in IPS engine	57
Resolved engine issues	57

Limitations	58
Citrix XenServer limitations	58
Open source XenServer limitations	58

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 27 and Known issues on page 51 .

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

Special notices

- [Azure-On-Demand image on page 8](#)
- [GCP-On-Demand image on page 8](#)
- [ALI-On-Demand image on page 8](#)
- [SSL traffic over TLS 1.0 will not be checked and will be bypassed by default on page 9](#)
- [Part numbers of unsupported FG-10xF, FGR-60F, and FGR-60F-3G4G Generation 2 models on page 9](#)
- [L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 on page 9](#)
- [Add interface for NAT46 and NAT64 to simplify policy and routing configurations on page 10](#)

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.

SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 and 6.4.3 ended support for TLS 1.0 when `strong-crypto` is enabled under `system global`. With this change, SSL traffic over TLS 1.0 will not be checked so it will be bypassed by default.

To examine and/or block TLS 1.0 traffic, an administrator can either:

- Disable `strong-crypto` under `config system global`. This applies to FortiOS 6.2.6 and 6.4.3, or later versions.
- Under `config firewall ssl-ssh-profile`:
 - in FortiOS 6.2.6 and later, set `unsupported-ssl` to `block`.
 - in FortiOS 6.4.3 and later, set `unsupported-ssl-negotiation` to `block`.

Part numbers of unsupported FG-10xF, FGR-60F, and FGR-60F-3G4G Generation 2 models

The following part numbers are Generation 2 models that do not support FortiOS 7.0.0:

- FG-100F-Gen2 P24589-20
- FG-101F-Gen2 P24605-20
- FGR-60F-Gen2 P25210-21
- FGR-60F-3G4G-Gen2 P25587-21

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

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 210.0.0.0
  set sip 210.0.0.255
  set status enable
  set usrgroup "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 "l2tp.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, 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

Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1, 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
<pre>config firewall vip46 edit "test-vip46-1" set extip 10.1.100.155 set mappedip 2000:172:16:200::55 next end</pre>	<pre>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</pre>

ippool6 object:

Old configuration	New configuration
<pre>config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 next end</pre>	<pre>config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 set nat46 enable next end</pre>

NAT46 policy:

Old configuration	New configuration
<pre>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</pre>	<pre>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</pre>

vip64 object

Old configuration	New configuration
<pre>config firewall vip64 edit "test-vip64-1" set extip 2000:10:1:100::155 set mappedip 172.16.200.155 next end</pre>	<pre>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</pre>

ippool object

Old configuration	New configuration
<pre>config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155 next end</pre>	<pre>config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155 set nat64 enable next end</pre>

NAT64 policy:

Old configuration	New configuration
<pre>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</pre>	<pre>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</pre>

Changes in CLI

Bug ID	Description
673049	<p>For <code>localid-type</code> address, unhide the <code>localid</code> option so customers have the option to set the ID directly for IPv4 or IPv6 addresses.</p> <pre>config vpn ipsec phase1 edit <name> set localid-type address set localid <string> next end</pre>
693347	<p>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.</p> <pre>config vpn ssl web portal edit <name> set ipv6-pools <address> set ipv6-split-tunneling-routing-address <address> next end</pre>
709109	<p>Add the following option to backup configuration files using SFTP:</p> <pre># execute backup config sftp <file name> <SFTP server><:SFTP port> [user] [password]</pre>
712794	<p>Allow the wireless controller to obtain temperature values from FortiAP-F models that have built-in temperature sensors:</p> <pre># diagnose wireless-controller wlac -c wtp <serial number> grep Temp</pre>

Changes in GUI behavior

Bug ID	Description
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 <i>SD-WAN</i> and <i>IPsec</i> 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	<p>Consolidates multiple NAT46/NAT64 related objects into regular objects, and introduce a per-VDOM virtual interface, <code>naf.<vdom></code>, that is automatically added to process NAT46/NAT64 traffic. The new changes and additions include:</p> <ul style="list-style-type: none">• Consolidate <code>vip46</code> and <code>vip64</code> setting into <code>vip</code> and <code>vip6</code> configurations.• Consolidate <code>policy46</code> and <code>policy64</code> settings into <code>firewall policy</code> settings.• Introduce <code>nat46/nat64</code> in <code>firewall policy</code> settings.• Extend <code>ippool</code> and <code>ippool6</code> to support NAT46 and NAT64.• Extend central SNAT to support NAT46 and NAT64.• Remove <code>firewall vip46/vip64</code>, <code>vipgrp46/vipgrp64</code>, and <code>policy46/policy64</code> settings.• Rename <code>system.nat64</code> to <code>system.dns64</code>. <p>To configure NAT46/NAT64 translation, users can use the standard <code>vip/vip6</code> setting, apply it in a firewall policy, enable NAT46/NAT64, and enter the IP pool to complete the configuration.</p>
699533	<p>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.</p>
709056	<p>Previously, the <code>tie-break fib-best-match</code> 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.</p>
718512	<p>Allow policy route match in the reply direction, and improve IPv6 route search for policy route to keep the same behavior as IPv4.</p>

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 <code>static6</code> table size from 500 per VDOM to 2000 per VDOM on FG-600-series models and higher.
713695	Increase central NAT rules (<code>firewall.central-snat-map</code>) 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	<p>Allow ingress and egress ports to be configured so the PRP trailer is not stripped when PRP packets come in or go out.</p> <pre>config system npu set prp-port-in <port> set prp-port-out <port> end</pre>
489956	<p>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).</p> <pre>config system npu set lag-out-port-select {enable disable} end</pre> <p>Add algorithm in NPU driver for distribution, AGG_ALGORITHM_NPU.</p>
568534	<p>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.</p> <p>VDOM level:</p> <pre>config switch-controller global set dhcp-server-access-list {enable disable} end</pre> <p>FortiSwitch level:</p> <pre>config switch-controller managed-switch edit <switch> set dhcp-server-access-list {global enable disable} next end</pre> <p>Interface:</p> <pre>config system interface edit <interface> config dhcp-snooping-server-list edit <list> set server-ip <class_ip> next end next end</pre>

Bug ID	Description
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.
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.
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.
696057	Add REST API to retrieve a list of FortiSwitch models that are supported on the FortiGate: <code>/api/v2/monitor/switch-controller/managed-switch/models</code>
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, <i>Switch Controller NAC Policy Tag</i> . This type of address can be assigned to a NAC policy under <i>Switch Controller Action</i> . 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. <pre># 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</pre>

Bug ID	Description
699456	Increase the generated RSA key bits from 1024 to 2048.
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. <pre> config system snmp sysinfo set engine-id-type {text hex mac} set engine-id <string, maximum 27 characters> end </pre>
702665	Add support for BGP conditional advertisement for IPv6 on the FortiGate: <pre> 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 </pre>
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: <ul style="list-style-type: none"> • 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 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.

Bug ID	Description
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 <code>push CA certs</code> 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.
707475	Enhancements for ZTNA logging: <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 1. <i>Network > SD-WAN > Performance SLA</i> tab: probe mode options are <i>Active</i>, <i>Passive</i>, or <i>Prefer Passive</i>. The disabled option can only be configured in the CLI. 2. In a <i>Firewall Policy</i> where the destination is a SD-WAN zone, the passive health check option is available. By enabling <i>Passive Health Check</i> in a policy, the TCP traffic for that policy will be used in health check measurements.
709061	In <i>WiFi & Switch Controller > Managed Switch > Topology View</i> , a new <i>Reorder</i> 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: <pre> config router key-chain edit <name> config key edit <id> set algorithm {md5 hmac-sha1 hmac-sha256 hmac-sha384 hmac-sha512} next end next end </pre>
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.

Bug ID	Description
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 <code>X-Forwarded-Client-Cert</code> 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 <i>Access Control and Authentication</i> to mitigate against the following high-priority vulnerability: <ul style="list-style-type: none"> LDAP Server Identity Check: ensures certificate validation takes place against LDAP server.
710323	Add security rating test in <i>Access Control and Authentication</i> to mitigate against the following high-priority vulnerability: <ul style="list-style-type: none"> 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 <i>Authorize</i> 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.
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.
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: <ol style="list-style-type: none"> Use the SD-WAN zone in IPv4 and IPv6 static routes. Use the SD-WAN zone in SD-WAN service rules. Add a pre-defined SD-WAN zone called SASE.
713535	Sniffer traffic logs from the IPS engine are expanded to 64-bit variable sizes (previously 32-bit for sent/received bytes fields).
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	<p>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:</p> <pre>config vpn ssl settings set saml-redirect-port <port> end</pre>
716453	On KVM, FortiOS can support bootstrapping using a MIME file via config drive.
716683	<p>FIPS CC mode is now supported on OCI and GCP FortiGate VMs.</p> <pre>config system fips-cc set status fips-ciphers end</pre> <p>To enable this feature, all VPNs must be removed.</p>
717579	<p>Add command in the WTP profile to disable console login from the FortiAP:</p> <pre>config wireless-controller wtp-profile edit <profile> set console-login {enable disable} next end</pre> <p>All managed APs using this profile will be rebooted and changes will be applied.</p>
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	<p>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:</p> <pre>config user fsso edit <name> set logon-timeout <integer> next end</pre> <p>The <code>logon-timeout</code> is measured in minutes (1 - 2880, default = 5).</p>
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.

Bug ID	Description
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.
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.

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 26
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiSandbox	• 2.3.3 and later, 4.0.0 is recommended

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 select *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *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) will support strong ciphers in the future release of version 5.4.3.

If FortiGates running FortiOS 7.0.1 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.

Product integration and support

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

Web browsers	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Microsoft Edge 44• Mozilla Firefox version 74• Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	<ul style="list-style-type: none">• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	<ul style="list-style-type: none">• 5.0 build 0301 and later (needed for FSSO agent support OU in group filters)<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 3.2.1
AV Engine	<ul style="list-style-type: none">• 6.00262
IPS Engine	<ul style="list-style-type: none">• 7.00029

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	<ul style="list-style-type: none"> 8.1 Express Edition, Dec 17, 2019
Linux KVM	<ul style="list-style-type: none"> Ubuntu 18.0.4 LTS Red Hat Enterprise Linux release 8.4 SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	<ul style="list-style-type: none"> 2012R2 with Hyper-V role
Windows Hyper-V Server	<ul style="list-style-type: none"> 2019
Open source XenServer	<ul style="list-style-type: none"> Version 3.4.3 Version 4.1 and later
VMware ESX	<ul style="list-style-type: none"> Versions 4.0 and 4.1
VMware ESXi	<ul style="list-style-type: none"> Versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7

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. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Anti Virus

Bug ID	Description
705591	When <code>av-scan</code> 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, <code>/tmp/cdr</code> 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 <code>analytics-wl-filetype</code> 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 <code>fnacd</code> .

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
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 <code>traffic-shaper</code> if <code>class-id</code> and <code>traffic-shaper</code> are both configured.
595949	Any changes to the security policy table causes the hit count to reset.
644225	Challenge ACK is being dropped.
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 <i>Last Used</i> information is different in the CLI and GUI.
694154	Dynamic traffic shapers are not consistent in their idle time limit.

Bug ID	Description
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 <code>policyid</code> .
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 <i>Failed to retrieve data</i> 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.
712580	When viewing FortiView <i>Sources</i> or <i>Destinations</i> , some usernames in the format of <code><DOMAIN\username></code> are displayed as <code>DOMAIN&bsol;username</code> . The user is displayed with a <code>\</code> in the CLI.
722543	FortiView does not arrange FortiGuard quota based on highest to lowest value and vice versa.

GUI

Bug ID	Description
585899	SAML auto configuration does not take <code>admin-sport</code> into account.
589231	Get <i>Invalid IP/Wildcard mask</i> . warning when editing the address object in the GUI.
602397	Managed FortiSwitch and FortiSwitch Ports pages are slow to load when there are many managed FortiSwitches.
610572	If a guest user logs in via a WiFi portal while the administrator is actively editing the user's account in the GUI, after the administrator clicks <i>OK</i> in the user edit dialog, the user's current login session will not be subjected to the configured expiration time. The expiration time will be applied for the next login.
645158	When logging into the GUI via FortiAuthenticator with two-factor authentication, the FortiToken Mobile push notification is not sent until the user clicks <i>Login</i> .
647431	After removing an image name on the <i>Replacement Messages Edit</i> page, an image list should be displayed when hovering the mouse over the image URL link, but it is not.
665597	When <code>set server-identity-check</code> is enabled, <i>Test User Credentials</i> 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 <i>Firewall Policy</i> , 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 <code>config ha-mgmt-interfaces</code> 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	httpsd has signal 6 and 11 crashes at <code>cmf_query_create_child</code> because of segfault in <code>/api/v2/monitor/switch-controller/managed-switch/transceivers</code> .
686592	GUI does not display statistical information on SD-WAN <i>Performance SLA</i> page.
689392	Port <i>Errors</i> 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 <i>Account Entitlement</i> when checking for FSAC contract.
695815	When editing the external connector <i>Poll Active Directory Server</i> from the GUI, the <i>Users/Groups</i> option is always an empty value, even if there is an existing group configured. The workaround is to manage the option from the CLI.
696226	<i>Network > Interfaces</i> page is slow to load.
696573	Firewall policy is not visible in GUI when using <code>set internet-service src enable</code> .

Bug ID	Description
701442	Cannot access GUI for FortiGate in FIPS-CC mode.
701742	Items added to <i>Favorites</i> 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 <code>default-allowed-methods</code> are not committed. The CLI must be used.
704209	When updating the <i>Disclaimer Page</i> replacement message, if the message is too long, the <i>Save</i> 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 the login banner is enabled and the user is forced to log in again to the GUI (due to password change or enabling VDOMs), the user may see a <i>Bad Gateway</i> error.
706340	When editing a firewall policy, copying and pasting in the <i>Comments</i> field gives an error.
706711	When <code>accprofile</code> is set to <code>fwgrp custom</code> with all read-write permissions, some GUI menus will not be visible. Affected menu items include <i>IP Pools</i> , <i>Protocol Options</i> , <i>Traffic Shapers</i> , and <i>Traffic Shaping Policy/Profile</i> .
706982	Unable to edit interface address, get <i>Bits of the IP address will be truncated by the subnet mask</i> 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.
709103	Unable to edit interfaces in the GUI, and <code>httpsd</code> is spiking the CPU cores.
709662	Static route for IPsec VPN shows tunnel ID as a gateway and provides an unreachable error.
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	<code>httpsd</code> process has high CPU and memory usages, causing the unit to enter conserve mode.
713580	Non-FortiToken RADIUS two-factor authentication not working when logging into the GUI.
715256	When the <i>Security Fabric Connection</i> is enabled on a VPN interface, the <i>DHCP Server</i> section disappears from the GUI.
715493	<code>httpsd</code> consumes high CPU when loading a GUI page.
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 <i>Unreachable or not authorized</i> .

Bug ID	Description
719620	Interface page keep loading when administrator user has <code>netgrp read-write</code> permissions only and interface contains IPsec VPN.
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 <code>hasync</code> 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 <i>Deny</i> contains unneeded lines.
703047	<code>hbdev</code> goes up and down quickly, then the cluster keeps changing rapidly. <code>hasync</code> objects might access invalid cluster information that causes it to crash.
703719	<code>hasync</code> is busy when receiving ARP when there is a huge number of ARPs in the network.
708928	The <code>set override disable</code> 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.
710236	Heartbeat interfaces do not get updated under <code>diagnose sys ha dump-by <group memory></code> after HA <code>hbdev</code> configuration changes.
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, <code>hataalk</code> will get a lot of <code>intf_vd_changed</code> events and recheck the MAC every time, which blocks <code>hataalk</code> 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.

Bug ID	Description
717251	In FGSP, <code>session-sync-dev</code> statistics of <code>get system ha status</code> 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 <code>ha-direct</code> .
721720	Performance degradation of session synchronization after upgrading.
722284	When there is a large number of VLAN interfaces (around 600), the FortiGate reports <code>VLAN heartbeat lost on subinterface vlan</code> error for multiple VLANs.

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.
673049	FortiGate is not sending its external interface IP in the IKE negotiation (cloud platform).
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.

Bug ID	Description
708940	When ADVPN with BGP has <code>routing-protocol</code> and <code>link-down-failover</code> 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 <code>Failed to find IPsec Common</code> 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 <code>net-device</code> 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.
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.
722315	System might generate garbage administrator log events upon session timeout.

Proxy

Bug ID	Description
663088	Application control in Azure fails to detect and block SSH traffic with proxy inspection.

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 <code>wad_async_queue</code> in FOH connect case.
683844	In cases when WAD fails to resolve a firewall policy for the session, WAD crashes at <code>wad_ssl_proxy_can_bypass()</code> when a missed condition check allows the session to still pass through.
700073, 714109	YouTube server added new URLs (<code>youtubei/v1/player</code> , <code>youtubei/v1/navigator</code>) 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 <code>wad_http_scan_engine__on_unblock</code> .
704323	In IPS TCP proxy handover, the firewall policy <code>tcp-mss-sender</code> , <code>tcp-mss-receiver</code> , and interface <code>tcp-mss</code> settings are not used.
706555	WAD crashes at <code>wad_ssl_port_p2s_set_server_cert</code> .
706556	WAD crashes at <code>wad_http_scan_safe_proc_msg</code> .
708514	WAD crash at <code>flush_sec_profile</code> after deleting VDOM.
709623	WAD crashes seen in user information upon user purge and during signal handling of user information history.
714610	Explicit proxy policy (ISDB and IP pool) cannot be set in the GUI or CLI.
719681	Flow control failure occurred while transferring large files when <code>stream-scan</code> 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.
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	<code>/api/v2/monitor/system/available-interfaces</code> 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.

Bug ID	Description
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.
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 (<i>Network > SD-WAN Rules</i> page).
688317	Blackhole route to the gateway of policy route makes the PBR inactive/disabled.
697645	FortiGate deletes <code>prefix-list</code> configuration due to concurrent administrator SSH sessions.
699122	Issues with SD-WAN zone's availability to select it as an OSPF interface.
701027	No speed test button for PPPoE interface in GUI on <i>Interfaces</i> 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 <i>Destination Host Unreachable</i> 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 <code>virtual-wan-link</code> 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	<i>Policy Routes</i> GUI page does not show red exclamation mark when a source or destination is negated, like on <i>Firewall Policy</i> page.
722343	SD-WAN rule not matched with MAC address object and ISDB in policy.

Bug ID	Description
723550	Load-balance service mode and maximize bandwidth (SLA) in SD-WAN rule does not work as expected in 7.0.0.
723726	BGP session drops between virtual wire pair with <code>auto-asic-offload</code> enabled in policy.
724250	Enabling <code>preserve-session-route</code> does not take effect in SD-WAN scenario.

Security Fabric

Bug ID	Description
672218	In multi-VDOM environment, when viewing logical topology under a specific VDOM view, the GUI incorrectly shows interfaces and devices from all VDOMs.
685642	Link to <i>Login to FortiAnalyzer on Physical Topology</i> 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.
714807	Security rating two-factor authentication test shows as failed for IPsec and SSL VPN, but all users have two-factor authentication enabled.
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 <code>%%log.date%%</code> and <code>%%log.time%%</code> 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 <code>script-src 'self'</code> will block the SSL VPN proxy URL.

Bug ID	Description
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: <i>Entry not found</i>).
676333	Unable to type accents using dead keys in RDP using Spanish keyboard layout over SSL VPN web mode in macOS.
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	sslvpn 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 (<i>no session matched</i>).
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.

Bug ID	Description
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.
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 <code>sslvpn_ppp_associate_fd_to_ipaddr</code> . 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.

Bug ID	Description
721427	Unable to load NetApp OnCommand Unified Manager webpages due to reloading loop in SSL VPN web mode.
724830	FortiGate sends authentication request to all RADIUS servers instead of only those in the default realm.
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 <code>fortilinkd</code> 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
568399	FG-200E has <code>np6lite_lacp_lifc</code> 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 <code>/api/v2/monitor/system/available-interfaces</code> (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 <code>..</code> can be created in the GUI, but it cannot be edited or deleted.
666418	SFP interfaces on FG-330xE do not show link light.

Bug ID	Description
667307	Console prints out NP6XLITE: np6xlite_hw_ipl_rw_mem_channel timeout message on SoC4 platforms.
671332	httpsd crashed after changing VDOM for interface.
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.
687398	Multiple SFPs and FTLX8574D3BCL in multiple FG-1100E units have been flapping intermittently with various devices.
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.
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.
703131	Split-task VDOM does not update IPS/AV from ha-direct connected internal FortiManager.
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.

Bug ID	Description
706131	When processing visibility log requests and passively learning FQDNs and wildcard FQDN addresses at a high rate, the CPU usage of dnstproxy can reach 90% or higher.
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 dhcpd 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 <code>execute private-encryption-key <xxx></code> .
714164	SNMP times out or has slow response when SNMP queries FortiGate session table OIDs.
714192	<code>diagnose sys bcm_intf cli "2:"</code> and <code>diagnose sys bcm_intf cli "ps"</code> 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 <code>drivers/net/macvlan.c:869</code>).
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 <code>ha monitor dev</code> .
715043	<i>Guest Management</i> page <i>Expire</i> 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.
715571	<code>config match</code> 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, <code>cmdbsvr</code> 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 <code>cmdbsvr</code> has finished sending it, but the last command is not yet stored in the auto update file.
717791	<code>execute restore vmlicense tftp</code> fails with <code>tftp: bind: Address already in use</code> .

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.
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 <code>set key-outbound</code> and <code>set key-inbound</code> parameters are missing for GRE tunnels under <code>config system gre-tunnel</code> .
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 <code>execute tac report</code> or <code>diagnose debug report</code> via SSH leaves a <code>tac_report*</code> file in <code>/tmp</code> .

Upgrade

Bug ID	Description
701571	After upgrading from 6.4.5 to 7.0.0, all flow-based policies are switched to proxy if there is a SIP profile attached to the firewall policy.
708250	Console prints <code>__set_clr_flag:wwan ioctl failed, flag:0x0200 errno:19</code> 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 <code>config system dns-database</code> , the <code>set type slave</code> configuration in 6.4.5 does not change to <code>set type secondary</code> 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 <code>allowaccess</code> 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 <i>Unable to connect to FortiGuard servers</i> 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.
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 wpa 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.
697058	Unable to change AP state under rogue AP's monitor page.

Bug ID	Description
698961	FWF-60F/61F and FWF-40F encounters kernel panic (<code>LR is at capwap_find_sta_by_mac</code>) 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.
709824	Dynamic VLAN SSID traffic cannot pass through VDOM link when <code>capwap-offload</code> 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	<code>get wireless-controller wtp-status</code> output only shows only one AP entry.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
712334	FortiOS7.0.1 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">CVE-2021-26110

Known issues

The following issues have been identified in version 7.0.1. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Application Control

Bug ID	Description
701926	Stress test with application control only results in packet drops.

Endpoint Control

Bug ID	Description
708545	The WAD daemon is triggered to fetch the FortiClient information based on a ZTNA EMS tag enabled for checking in a proxy policy. It is then possible to get a ZTNA EMS tag in the firewall dynamic address and get the expected traffic control.
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
719311	FortiGate is partially not showing policies after upgrading from 6.2.7.

GUI

Bug ID	Description
677806	State of IPsec tunnel interfaces that do not belong to the management VDOM show up in global view.

Bug ID	Description
685431	GUI policy page takes around 30 seconds to load 24K policies.
699508	Administrator logout log does not reflect the correct timeout setting if the administrator closes the browser directly.
701367	Statistics of <code>vcluster2</code> are not shown in the GUI.
707589	<i>System > Certificates</i> list sometimes shows 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.
708947	Policy dialogs (firewall, NAT46, NAT64, proxy) sometimes get stuck loading due to an error when generating a security rating report. Workaround: manually re-run the security rating report from the <i>Security Fabric > Security Rating</i> page.
714304	Firewall policies configured in the CLI can contain special characters (<, >, (,), #, ', ") in the name, but these characters are invalid when configuring a policy in the GUI.
720613	Sometimes the event log is duplicated when downloaded from the GUI.
720657	Unable to set link local address in GUI.
722832	When LDAPS is configured with FQDN and a server identity check, all LDAP-related GUI pages do not work. The CLI and <code>fnband</code> are OK.

HA

Bug ID	Description
694984	Session count of UDP traffic gradually decreases on the secondary unit in a FGSP-TP cluster.
695067	When there are more than two members in a HA cluster and the HA interface is used for the heartbeat interface, some RX packet drops are observed on the HA interface. However, no apparent impact is observed on the cluster operation. Workaround: do not use the HA interface as a heartbeat interface.
717788	FGSP has problem at failover when NTurbo or offloading is enabled (IPv4).

Intrusion Prevention

Bug ID	Description
669089	IPS profile dialog in GUI shows misleading <i>All Attributes</i> in the <i>Details</i> field for filter entries with a CVE value.

IPsec VPN

Bug ID	Description
668997	<i>Duplicate entry found</i> error shown when assigning multiple dial-up IPsec tunnels with the same secondary IP in the GUI.
699973	IPsec aggregate shows as down on <i>Interfaces</i> , <i>Firewall Policy</i> , and <i>Static Routes</i> configuration pages.
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	<p>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:</p> <ul style="list-style-type: none"> Using <code>set gateway enable</code> in a particular SD-WAN service Having <code>mode-cfg</code> configured Not having ADVPN configured on the hub <p>Workaround: Before upgrading, update the hub and spoke configurations as follows:</p> <ul style="list-style-type: none"> On the hub, enable the <code>exchange-interface-ip</code> option on the dial-up phase1 interface with <code>mode-cfg</code> configured. On the spoke, enable <code>auto-discovery-receiver</code> on the related phase1 interface.

Proxy

Bug ID	Description
712584	WAD memory leak causes device to go into conserve mode.

REST API

Bug ID	Description
731136	<p>The following API has a change in response format, which may break backward compatibility for existing integration:</p> <pre>POST /api/v2/monitor/system/config/restore</pre> <p>New format results: <code>{'config_restored': True}</code></p> <p>Old format results: <code>{'restore_started': True, 'session_id': 'nTuRkV'}</code></p> <p>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.</p>

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
726831	Security rating for <i>Local Log Disk Not Full</i> reporting as failed for FortiGate models without log disks.

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
639861	Support FEC (forward error correction) implementations in 10G, 25G, 40G, and 100G interfaces for FG-3400E and FG-3600E.
644616	NP6 does not update session timers for traffic IPsec tunnel if established over one pure EMAC VLAN interface.
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
675558	SFP port with 1G copper SFP always is up.
679035	NP6 drops, and bandwidth limited to under 10 Gbps.
683299	Port group members have different speeds after the port speed is changed using a CLI script.
685674	FortiGate did not restart after restoring backup configuration.
698003	When creating a new administrator, the administrator profile's reference is visible in other administrator accounts from different VDOMs.
706686	LAG interface between FortiGate and Cisco switch flaps when adding/removing member interface.
710635	GUI should hide the <i>FortiGate Setup</i> dialog if all setup steps are complete.
713835	The BLE pin hole behavior should not be applied on FG-100F generation 1 that has no BLE built in.
721487	FortiGate often enters conserve mode due to high memory usage by httpsd process.

User & Authentication

Bug ID	Description
707057	TACACS server traffic will not go through the specific interface from the GUI irrespective of the interface set under the TAC.
725056	FSSO local poller fails after recent Microsoft Windows update (KB5003646, KB5003638, ...).

VM

Bug ID	Description
689047	ARM64-KVM has kernel panic.
721439	Problems occur when switching between HA broadcast heartbeat to unicast heartbeat and vice versa.
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 <code>execute factoryreset2</code> on the secondary instance, and reconfigure the auto scaling group.

WAN Optimization

Bug ID	Description
728861	HTTP/HTTPS traffic cannot go through when <code>wanopt</code> is set to manual mode and an external proxy is used. Workaround: set <code>wanopt</code> to automatic mode, or set <code>transparent disable</code> in the <code>wanopt</code> profile.

WiFi Controller

Bug ID	Description
700356	CAPWAP daemon crashing due to IoT detection.
719217	Interface <i>Bandwidth</i> widget should exclude bridge VAP interface (and mesh VAP interface).

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 <code>load_SearchFile</code> ; 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, <code>/tmp/cdr</code> is not cleaned after a scan when there are multiple concurrent sessions.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
654356	In NGFW policy mode, sessions are not re-validated when security policies are changed. A workaround is to clear sessions after a policy change.
672994	Web filter warning message does not contain certification chain.
673117	TFTP traffic does not work well when TFTP application is set in security policy.
681611	IPS engine crashes (5.218 <code>ips_dlp_alert</code>).
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.
707907	IPS engine (flow mode deep inspection) does not decrypt some TLS 1.3 sessions, which causes problems with application control detection.
713068	FGSP support in NGFW policy mode.
715136	High memory usage for some slab objects.
718452	<code>set https-replacemsg disable</code> causing connection RST on URLs in URL filter list (flow-based inspection).
719007	URL filtering followed by <code>/*</code> causes rating error.
719252	IPS engine crash.
720605	URL filter with exempt setting does not avoid anti virus and IPS inspection.
721410	Unable to open fb.watch website in flow mode using SSL deep inspection with application control.
721462	Memory usage increases up to conserve mode after upgrading IPS engine to 5.00239.
724400	Facebook.com website gives error in Firefox version 89 with flow mode and deep inspection.
724767	Hostname is garbled in event log that is detected by <code>HTTP.Suspicious.Headers.With.Special.Characters</code> .
729249	Web filter categorizes private IP address and local URLs as <code>Newly Observed Domain</code> .

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

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.