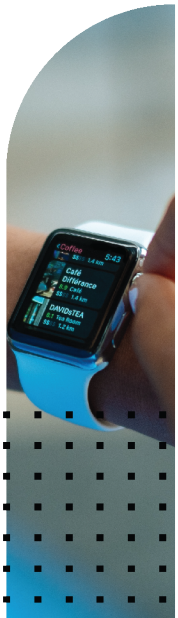
Release Notes

FortiOS 7.0.7



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

October 06, 2022
FortiOS 7.0.7 Release Notes
01-707-848454-20221006

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-10-06	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.0.7 build 0367.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.7 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-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, 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-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-ARM64-AWS, FG-ARM64-KVM, 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

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.

Unsupported websites in SSL VPN web mode

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

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

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

CAPWAP offloading compatibility of FortiGate NP7 platforms

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

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

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

FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
    edit <id>
        set fec enable
    next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.

Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.0.7 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4201F). These FortiGates can also be licensed for hyperscale firewall features. Previous versions of FortiOS supported FortiGates with NP7 processors through special branch firmware builds.

For more information, refer to the Hyperscale Firewall Release Notes.

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

FortiAnalyzer	• 7.0.3
FortiManager	• 7.0.3
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 12
FortiClient* EMS	• 7.0.0 build 0042 or later
FortiClient* Microsoft Windows	• 7.0.0 build 0029 or later
FortiClient* Mac OS X	• 7.0.0 build 0022 or later
FortiClient* Linux	• 7.0.0 build 0018 or later
FortiClient* iOS	• 6.4.6 build 0507 or later
FortiClient* Android	• 6.4.6 build 0539 or later
FortiSandbox	• 2.3.3 and later

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

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

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

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.7. When Security Fabric is enabled in FortiOS 7.0.7, all FortiGate devices must be running FortiOS 7.0.7.

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): version 5.4.3 and later

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.

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

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

To make L2TP over IPsec work after upgrading:

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

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

   Add a static route after upgrading:

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

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

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

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

Upgrading

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

The following CLI commands have been removed:

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

The following GUI pages have been removed:

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

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

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

The following output is displayed after running the diagnose command:

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

Creating new policies

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

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

Example configurations

`vip46` object:

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

`ippool6` object:

Old configuration	New configuration
config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 next end	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

NAT46 policy:

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

`vip64` object

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

`ippool` object

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

NAT64 policy:

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

ZTNA configurations and firewall policies

Since FortiOS 7.0.2, ZTNA configurations no longer require a firewall policy to forward traffic to the access proxy VIP. This is implicitly generated based on the ZTNA rule configuration.

When upgrading from FortiOS 7.0.1 or below:

- If an `access-proxy` type `proxy-policy` does not have a `srcintf`, then after upgrading it will be set to `any`.
- To display the `srcintf` as *any* in the GUI, *System* > *Feature Visibility* should have *Multiple Interface Policies* enabled.
- All full ZTNA firewall policies will be automatically removed.

Default DNS server update

If both primary and secondary DNS servers are set to use the default FortiGuard servers prior to upgrading, the FortiGate will update them to the new servers and enable DoT after upgrading. If one or both DNS servers are not using the default FortiGuard server, upgrading will retain the existing DNS servers and DNS protocol configuration.

Product integration and support

The following table lists FortiOS 7.0.7 product integration and support information:

Web browsers	• Microsoft Edge • Mozilla Firefox version 100 • Google Chrome version 101 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C

Fortinet Single Sign-On (FSSO)	• 5.0 build 0306 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 Core (requires Microsoft SHA2 support package)
	  • Novell eDirectory 8.8

AV Engine	• 6.00276
IPS Engine	• 7.00126

Virtualization environments

The following table lists hypervisors and recommended versions.

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

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 100 Google Chrome version 101
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 100 Google Chrome version 101
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 100 Google Chrome version 101
macOS Monterey 12.4	Apple Safari version 15 Mozilla Firefox version 100 Google Chrome version 101
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 7.0.7. For inquires about a particular bug, please contact Customer Service & Support.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
846234	FortiOS 7.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684
846854	FortiOS 7.0.7 is no longer vulnerable to the following CVE Reference: • CVE-2022-40684

Known issues

The following issues have been identified in version 7.0.7. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
727067	FortiGate should fix the interface between FortiGate and FortiAnalyzer for the CDR file.
795784	Able to bypass FortiOS AV inspection on email traffic when manipulating a MIME attachment with junk and pad characters in Base64.
800731	Flow AV sends HTML files to the FortiGate Cloud Sandbox every time when HTML is not configured in file list.
805655	A scanunit crash with signal 11 occurs for SMTP and QP encoding.

Endpoint Control

Bug ID	Description
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. **Workaround**: delete the EMS Cloud entry then add it back.
775742	Upgrade EMS tags to include classification and severity to guarantee uniqueness.

Firewall

Bug ID	Description
824091	Promethean Screen Share (multicast) is not working on the member interfaces of a software switch.

FortiView

Bug ID	Description
804177	When setting the time period to *now* filter, the table cannot be filtered by policy type.
811095	Threat type *N/A - Static URL Filter* is showing on sources that do not have the URL filter enabled.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.
707589	*System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. **Workaround**: use Chrome, Edge, or Safari as the browser.
749843	*Bandwidth* widget does not display traffic information for VLAN interfaces when a large number of VLAN interfaces are configured.
755177	When upgrade firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
777145	*Managed FortiSwitches* page incorrectly shows a warning about an unregistered FortiSwitch even though it is registered. This only impacts transferred or RMAed FortiSwitches. This is only a display issue with no impact on the FortiSwitch's operation. **Workaround**: confirm the FortiSwitch registration status in the FortiCare portal.
798161	*System* > *Certificates* page keeps spinning when trying to access it from Safari.
810225	An *undefined* error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
831885	Unable to access GUI via HA management interface of secondary unit.

HA

Bug ID	Description
750978	Interface link status of HA members go down when `cfg-revert` tries to reboot post `cfg-revert-timeout`.
782734	Cluster is out-of-sync due to switch controller managed switch checksum mismatch.
785514	In some situations, the fgfmd daemon is blocked by a query to the HA secondary checksum, which causes the tunnel between the FortiManager and FortiGate to go down.
803354	After HA-AP failover, the FortiExtender WAN interface of the new primary cannot get the LTE IP address from FortiExtender.
810286	FGSP local sessions exist after rebooting an HA pair with A-P mode, and the HW SSE/session count is incorrect.
811535	HA failure occurs on pair of FG-2600s due to packet loss on heartbeat interface.
830463	After shutting down the HA primary unit and then restarting it, the uptime for both nodes is zero, and it fails back to the former primary unit.

Hyperscale

Bug ID	Description
804742	After changing hyperscale firewall policies, it may take longer than expected for the policy changes to be applied to traffic. The delay occurs because the hyperscale firewall policy engine enhancements added to FortiOS 7.0.6 may cause the FortiGate to take extra time to compile firewall policy changes and generate a new policy set that can be applied to traffic by NP7 processors. The delay is affected by hyperscale policy set complexity, the total number of established sessions to be re-evaluated, and the rate of receiving new sessions.
805846	In the FortiOS MIB files, the trap fields `fgFwIppStatsGroupName` and `fgFwIppStatsInusePBAs` have the same OID. As a result, the `fgFwIppStatsInusePBAs` field always returns a value of `0`.
807476	After packets go through host interface TX/RX queues, some packet buffers can still hold references to a VDOM when the host queues are idle. This causes a VDOM delete error with `unregister_vf`. If more packets go through the same host queues for other VDOMs, the issue should resolve by itself because those buffers holding the VDOM reference can be pushed and get freed and recycled.
810025	Using EIF to support hairpinning does not work for NAT64 sessions.
810379	Creating an access control list (ACL) policy on a FortiGate with NP7 processors causes the npd process to crash.

Bug ID	Description
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.
812833	FortiGate still holds `npu-log-server` related configuration after removing hyperscale license.
836976	Traffic impact on changing from log to hardware to log to host during runtime (with PPA enabled).
837270	Disabling *Block intra-zone traffic* in a zone does not allow TCP/UDP traffic between interfaces of a zone.
838654	Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic.
839958	`service-negate` does not work as expected in a hyperscale deny policy.
842008	After HA failover, session count cannot synchronize on secondary FortiGate.
843197	Output of `diagnose sys npu-session list/list-full` does not mention policy route information.
843266	Diagnose command should be available to show `hit_count/last_used` for policy route and NPU session on hyperscale VDOM.
843305	Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when system boots up.
846520	NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover.

IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.
790486	Support IPsec FGSP per tunnel failover.
810988	GUI does not allow IP overlap for a tunnel interface when `allow-subnet-overlap` is enabled (CLI allows it).
815253	NP7 offloaded egress ESP traffic that was not sent out of the FortiGate.
815969	Cannot apply dialup IPsec VPN settings modifications in the GUI when `net-device` is disabled.

Log & Report

Bug ID	Description
790893	Logging filters do not work as expected.

Bug ID	Description
814427	FortiGate error in FortiAnalyzer connectivity test on secondary device after upgrade.
821359	FortiGate appears to have a limitation in the syslogd filter configuration.

Proxy

Bug ID	Description
768278	WAD crashes frequently, authentication stops, and firewall freezes once proxy policy changes are pushed out.
793651	An expired certificate can be chosen when creating an SSL/SSH profile for deep inspection.
809346	FTPS helper is not opening pinholes for expected traffic for non-standard ports.
823247	WAD user_info process leaks memory.

Routing

Bug ID	Description
756955	Routing table does not reflect the new changes for the static route until the routing process is restarted when cmdbsrv and other processes take CPU resources upon every configuration change in devices with over ten thousand firewall policies.
795213	On the *Network* > *SD-WAN* page, adding a named static route to an SD-WAN zone creates a default blackhole route.
796070	Incorrect SD-WAN kernel routes are used on the secondary device.
796409	GUI pages related to SD-WAN rules and performance SLA take 15 to 20 seconds to load.
808840	After cloning a static route, the URL gets stuck with `"clone=true"`.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
794703	Security Rating report for *Rogue AP Detection* and *FortiCare Support* checks show incorrect results.

Bug ID	Description
803600	Automation stitch for a scheduled backup is not working.
814796	The threat level threshold in the compromised host trigger does not work.
815984	Azure SDN connector has a 403 error when the AZD restarts.

SSL VPN

Bug ID	Description
626311	SSL VPN users are remaining logged on past the `auth-timeout` value.
767832	After upgrading from 6.4.7 to 7.0.1, the `Num Lock` key is turned off on the SSL VPN webpage.
780765	High CPU usage in SSL VPN using libssh2.
789642	Unable to load Grafana application through SSL VPN web mode.
796768	SSL VPN RDP is unable to connect to load-balanced VMs.
809209	SSL VPN process memory leak is causing the FortiGate to enter conserve mode over a short period of time.
809473	When sslvpnd debugs are enabled, the SSL VPN process crashes more often.
810715	Web application is not loading in the SSL VPN web mode.
811007	The auto-generated URL on the *VPN* > *SSL-VPN Settings* page shows the management IP of the FortiGate instead of the SSL VPN interface port IP as defined on the *VPN* > *SSL-VPN Realms* page when a realm is created.
811492	SSL VPN should not leak information while performing Telnet.
814040	SSL VPN bookmark configuration is added automatically after client logs in to web mode.
814708	The same SAML user failed to establish a tunnel when a stale web session exists with `limit-user-logins` enabled.
816716	sslvpnd crashed when deleting a VLAN interface.
816881	TX packet loss on ssl.root interface.
817843	Logging out of SSL VPN tunnel mode does not clear the authenticated list.
819296	GUI should not use <server_ip> as a sender to send the SSL VPN configuration (it should use value set in `reply-to`).

Switch Controller

Bug ID	Description
794026	FortiGates quarantines are stuck at 256.
803307	The *Enable STP* security control description should be reworded to mention that Edge ports should have STP enabled once the network topology is stable.
805154	Switch controller preconfiguration of FortiSwitch 108F-POE is incorrect.
810550	Send DHCP/ARP packet failed, and get `errno = 6` in log when `config-sync` runs.

System

Bug ID	Description
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected.
751870	User should be disallowed from sending an alert email from a customized address if the email security compliance check fails.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.
764954	FortiAnalyzer serial number automatically learned from miglogd does not send it to FortiManager through the automatic update.
787595	FFDB cannot be updated with `exec update-now` or `execute internet-service refresh` after upgrading the firmware in a large configuration.
789153	A profile with higher privileges than the user's own profile can be set.
798091	After upgrading from 6.4.9 to 7.0.5, the FG-110xE's 1000M SFP interface may fail to auto-negotiate and cannot be up due to the missed auto-negotiation.
798303	The threshold for conserve mode is lowered.
800294	Interface migration wizard fails to migrate interfaces when VLANs have dependencies within dependencies.
801053	FG-1800F existing hardware switch configuration fails after upgrading.
807947	Unable to create new interface and VDOM link with names that contain spaces.
813223	Random kernel panic occurs due to calling `timer_setup`.
815360	NP7 platforms may encounter a kernel panic when deleting more than two hardware switches at the same time.
819640	SSH public key changes after every reboot.

Bug ID	Description
824464	CMDB checksum is not updated when a certificate is renewed over CMP, causing a FortiManager failure to synchronize with the certificate.

Upgrade

Bug ID	Description
803041	Link lights on the FG-1100E fail to come up and are inoperative after upgrading.

User & Authentication

Bug ID	Description
813407	Captive portal authentication with RADIUS user group truncates the token code to eight characters.

VM

Bug ID	Description
786278	Bandwidth usage is not shown when DPDK is enabled.
803219	Azure SDN connector might miss dynamic IP addresses due to only the first page of the network interface being processed.
809963	Get cmdbsvr crash on FG-KVM32 after running concurrent performance test.

WAN Optimization

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

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.

WiFi Controller

Bug ID	Description
796036	Manual quarantine for wireless client connected to SSID on multi-VDOM with `wtp-share` does not work.
807713	FortiGate is not sending RADIUS accounting message consistently to RADIUS server for wireless SSO.
809623	CAPWAP traffic is dropped when `capwap-offloading` is enabled.
811953	Configuration installation from FortiManager breaks the quarantine setting, and the VAP becomes undeletable.
821803	Wireless multicast traffic causes the cw_acd process to have high CPU usage and triggers a hostapd crash.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
590623	Strange padding occurs in certificate after deep inspection (`ICAgICAg...`).
673117	TFTP traffic does not work well when TFTP application is set in security policy.
687885	Inconsistent system performance with RFC 2544 Ixia BreakingPoint testing.
757322	Inconsistent system performance with RFC 2544 Ixia BreakingPoint testing using frame size 68 and SR-IOV interface.
781110	Lost packets with security (UTM) profiles and third party WAN optimizer (Riverbed).
789861	Globus file transfer traffic breaks when web filter profile is enabled along with certificate inspection.
791175	Unable to access specific website after upgrading the IPS engine version.
798961	High CPU usage occurs on all cores in system space in __posix_lock_file for about 30 seconds when updating the configuratrion or signatures.
800524	IPS engine version 6.004.114 has crash with signal 11.
800730	When using NGFW policy based mode, modifying a security policy causes all sessions to be reset.
800731	Flow mode AV sends HTML files every time to the FortiGate Cloud Sandbox when it is not configured in the file list.
802683	IPS debug filter is not working.
804500	Changes to the custom URL filter cause a network degradation that impacts customers.
810105	Signal 14 (alarm clock) received when updating and during hasync crash.
811551	Traffic drop in NGFW mode post upgrading.
816032	Security policy with FSSO authentication sporadically does not match.
816759	IPS engine 5.00272 crash on `ovrd_ssl_read`.
817902	IPS engine 6.004.128 crashes with signal 11.
827253	Only traffic to pure IPv6 is blocked, and traffic to obfuscated IPv6 is not detected by FortiOS.
839679	PS engine version 6.004.139 has crash with signal 11.
840232	The hostname in syslog is short.
841269	When using SSL certificate inspection, no block page appears when application control and web filter are enabled on the same policy.

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