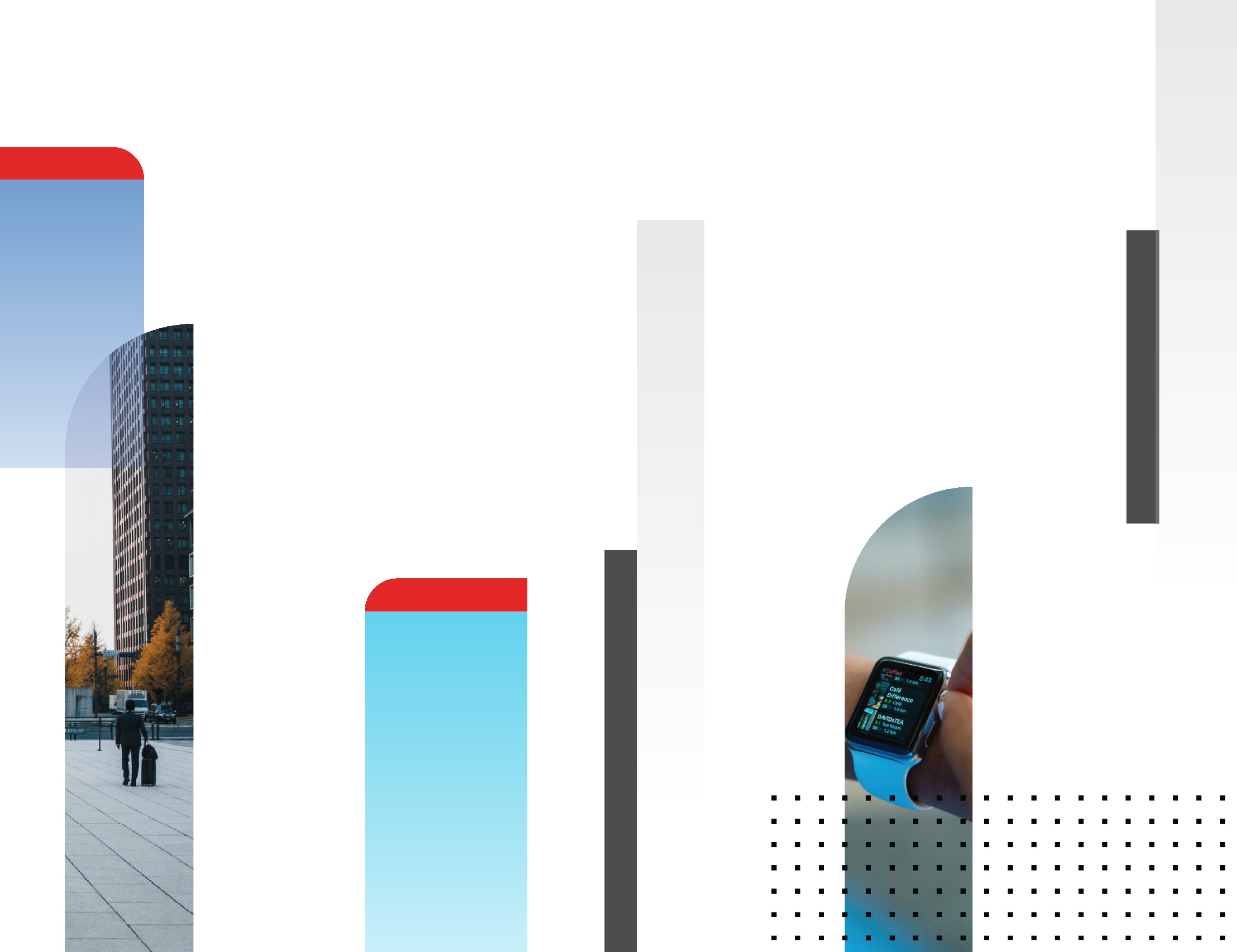
Release Notes

FortiOS 7.0.16



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

October 22, 2024
FortiOS 7.0.16 Release Notes
01-7015-1079805-20241022

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-10-22	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.0.16 build 0667.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.16 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-70F, FG-71F, 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-400F, FG-401F, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, 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-3000F, FG-3001F, 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
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-KVM, FG-ARM64-OCI, 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 branch supported models

The following models are released on a special branch of FortiOS 7.0.16. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0667.

FG-80F-DSL	is released on build 7518.
FG-90G	is released on build 7535.

FG-91G	is released on build 7535.
FG-120G	is released on build 7536.
FG-121G	is released on build 7536.
FG-900G	is released on build 7517.
FG-901G	is released on build 7517.
FG-1000F	is released on build 7523.
FG-1001F	is released on build 7523.
FG-3200F	is released on build 7528.
FG-3201F	is released on build 7528.
FG-3700F	is released on build 7528.
FG-3701F	is released on build 7528.
FG-4800F	is released on build 7528.
FG-4801F	is released on build 7528.
FGR-70F	is released on build 7515.
FGR-70F-3G4G	is released on build 7515.
FWF-80F-2R-3G4G-DSL	is released on build 7518.
FWF-81F-2R-3G4G-DSL	is released on build 7518.

Special notices

- Upgrading from older firmware versions on page 9
- Azure-On-Demand image on page 9
- GCP-On-Demand image on page 10
- ALI-On-Demand image on page 10
- Unsupported websites in SSL VPN web mode on page 10
- RDP and VNC clipboard toolbox in SSL VPN web mode on page 10
- CAPWAP offloading compatibility of FortiGate NP7 platforms on page 10
- IP pools and VIPs are now considered local addresses on page 11
- FEC feature design change on page 11
- Hyperscale incompatibilities and limitations on page 11
- SMB drive mapping with ZTNA access proxy on page 12
- Remote access with write rights through FortiGate Cloud on page 12
- Hyperscale NP7 hardware limitation on page 12
- HA unsupported between different FortiGate 90G and 91G series hardware generations on page 12

Upgrading from older firmware versions

It is best practices to use the Upgrade Path Tool to find the recommended upgrade path before performing an upgrade. Additionally, please refer to the following Upgrade Notices for a smooth upgrade.

- GUI firmware upgrade does not follow the recommended upgrade path on page 26
- Upgrading from 7.0.11 or earlier versions on page 26

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 and later:

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

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

CAPWAP offloading compatibility of FortiGate NP7 platforms

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

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later

- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

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

IP pools and VIPs are now considered local addresses

In FortiOS 7.0.13 and later, all IP addresses used as IP pools and VIPs are now considered local IP addresses if responding to ARP requests on these external IP addresses is enabled (`set arp-reply enable`, by default). For these cases, the FortiGate is considered a destination for those IP addresses and can receive reply traffic at the application layer.

Previously in FortiOS 7.0.1 to 7.0.12, this was not the case. For details on the history of the behavior changes for IP pools and VIPs, and for issues and their workarounds for the affected FortiOS versions, see Technical Tip: IP pool and virtual IP behavior changes in FortiOS 6.4, 7.0, 7.2, and 7.4.

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.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.0.16 features.

SMB drive mapping with ZTNA access proxy

In FortiOS 7.0.12 and later, SMB drive mapping on a Windows PC made through a ZTNA access proxy becomes inaccessible after the PC reboots when access proxy with TCP forwarding is configured as FQDN. When configured with an IP for SMB traffic, same issue is not observed.

One way to solve the issue is to enter the credentials into Windows Credential Manager in the form of `domain\username`.

Another way to solve the issue is to leverage the KDC proxy to issue a TGT (Kerberos) ticket for the remote user. See ZTNA access proxy with KDC to access shared drives for more information. This way, there is no reply in Credential Manager anymore, and the user is authenticated against the DC.

Remote access with write rights through FortiGate Cloud

Remote access with read and write rights through FortiGate Cloud now requires a paid FortiGate Cloud subscription. The FortiGate can still be accessed in a read-only state with the free tier of FortiGate Cloud. Alternatively, you can access your FortiGate through its web interface.

Please contact your Fortinet Sales/Partner for details on purchasing a FortiGate Cloud Service subscription license for your FortiGate device.

For more information see the FortiGate Cloud feature comparison and FortiGate Cloud Administration guide FAQ.

Hyperscale NP7 hardware limitation

Because of an NP7 hardware limitation, for CGN traffic accepted by a hyperscale firewall policy that includes an overload with port block allocation (overload PBA) IP Pool, only one block is allocated per client. The setting of the hyperscale firewall policy `cgn-resource-quota` option is ignored.

Because of this limitation, under certain rare conditions (for example, only a single server side IP address and port are being used for a large number of sessions), port allocation may fail even if the block usage of the client is less than its quota. In cases such as this, if the client has traffic towards some other servers or ports, additional port allocation can become successful. You can also work around this problem by increasing the IP Pool block size (`cgn-block-size`).

HA unsupported between different FortiGate 90G and 91G series hardware generations

Because of significant differences in interface naming conventions between Generation 1 and Generation 2 FortiGate 90G and 91G series devices, the high availability (HA) feature is not supported between Generation 1 and Generation 2 of the same devices.

For example, for a Generation 1 FortiGate 91G device, the following output is observed:

```
FortiGate-91-Gen1 # get hardware status
Model name: FortiGate-91G
ASIC version: SOC5
CPU: ARMv8
Number of CPUs: 8
RAM: 7547 MB
EMMC: 9982 MB(MLC) /dev/mmcblk0
Hard disk: 114473 MB /dev/nvme0n1
USB Flash: not available
Network Card chipset: FortiASIC NP7LITE Adapter (rev.)
Hardware Board ID: 002
```

For a Generation 2 FortiGate 91G device, the following output is observed:

```
FortiGate-91G-Gen2 # get hardware status
Model name: FortiGate-91G
ASIC version: SOC5
CPU: ARMv8
Number of CPUs: 8
RAM: 7547 MB
EMMC: 9982 MB(MLC) /dev/mmcblk0
Hard disk: 114473 MB /dev/nvme0n1
USB Flash: 58991 MB
Network Card chipset: FortiASIC NP7LITE Adapter (rev.)
Hardware Board ID: 003
```

Observe the Generation differences are reflected in the differences in *Hardware Board ID*.

In this example, for the Generation 1 FortiGate 91G, the WAN interfaces are `wan1` and `wan2`, respectively. However, for the Generation 2 FortiGate 91G, the WAN interfaces are `x1` and `x2`, respectively. Therefore, because of the differences in interface names, HA cannot be formed between these Generation 1 and Generation 2 devices.

Changes in default behavior

Bug ID	Description
1006011	Starting 7.4.4, FMG-Access is no longer enabled by default on all interfaces. In the event of an upgrade from a previous version, if the `central-management` type is not set as FortiManager, the `fgfm` will be disabled across all interfaces.

New features or enhancements

More detailed information is available in the New Features Guide.

Feature ID	Description
480717	Add new command to all FortiGate models that have dedicated management (mgmt, mgmt1, mgmt2) ports. `config system dedicated-mgmt`
685910	Added SoC4 driver support for the IEEE 802.1ad, also known as QinQ.
846399	Added 100G speed option for FG180xF for ports 37/38/39/40. Upon firmware upgrade, existing port speeds are preserved that have already been configured.
930522	Remote access with read and write rights through FortiGate Cloud now requires a paid FortiGate Cloud subscription. The FortiGate can still be accessed in a read-only state with the free tier of FortiGate Cloud. Alternatively, you can access your FortiGate through its web interface. Please contact your Fortinet Sales/Partner for details on purchasing a FortiGate Cloud Service subscription license for your FortiGate device.

936747	On FortiGates with multiple NP7 processors with hyperscale enabled, you can use the following command to optimize NP7 network session setup (NSS) engine performance.
	`config system npu`
	`    set nss-threads-option {4T-EIF | 4T-NOEIF | 2T}`
	`end`
	• `4T-EIF`: the NSS is configured with four threads and the Endpoint Independent Filtering (EIF) feature is allowed (the default). NSS with four threads supports the maximum NP7 Connections Per Second (CPS) performance.
	• `4T-NOEIF`: the NSS is configured with four threads and the EIF feature is not allowed. Also supports the maximum NP7 CPS performance.
	• `2T`: the NSS is configured with two threads and the EIF feature is allowed. This setting reduces the maximum NP7 CPS performance.
	Changing the `nss-threads-option` causes the FortiGate to restart.

1006448	Enhanced SSL VPN security by restricting and validating HTTP messages that are used only by web mode and tunnel mode.
1012626	In this enhancement, a hash of all executable binary files and shared libraries are taken during image build time. The file containing these hashes, called the executable hash, is also hashed, and as a result, signed. The signature for this hash is verified during bootup to ensure integrity of the file. After validation, the hashes of all executable and share libraries can be loaded into memory for real-time protection.

Feature ID	Description
1013511	This enhancement requires the kernel to verify the signed hashes of important file-system and object files during bootup. This prevents unauthorized changes to file-systems to be mounted, and other unauthorized objects to be loaded into user space on boot-up. If the signed hash verification fails, the system will halt.

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

FortiAnalyzer	• 7.0.13
FortiManager	• 7.0.13
FortiExtender	• 7.0.3 and later. For compatibility with latest features, use latest 7.4 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 19
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.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.0.0, use FortiClient 7.0.0.

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/FortiNDR
19. FortiTester
20. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.16. When Security Fabric is enabled in FortiOS 7.0.16, all FortiGate devices must be running FortiOS 7.0.16.

Downgrading to previous firmware versions

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

- operation mode
- interface IP/management IP
- static route table
- DNS settings

- admin user account
- session helpers
- system access profiles

Firmware image checksums

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

IPsec interface MTU value

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

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

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

HA role wording changes

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

Strong cryptographic cipher requirements for FortiAP

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

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

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

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

How VoIP profile settings determine the firewall policy inspection mode

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

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

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

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

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

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

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

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

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

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

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

To make L2TP over IPsec work after upgrading:

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

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

   Add a static route after upgrading:

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

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

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

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

Upgrading

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

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`

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

The following GUI pages have been removed:

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

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

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

The following output is displayed after running the diagnose command:

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

Creating new policies

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

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

Example configurations

`vip46` object:

Old configuration	New configuration

`config firewall vip46`
`    edit "test-vip46-1"`
`        set extip 10.1.100.155`
`        set mappedip 2000:172:16:200::55`
`    next`
	`config firewall vip`
	`    edit "test-vip46-1"`
	`        set extip 10.1.100.150`
	`        set nat44 disable`
	`        set nat46 enable`

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

Old configuration	New configuration

end	**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

Starting in FortiOS 7.0.4, 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.

VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later
- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

BIOS-level signature and file integrity checking during downgrade

When downgrading to a version of FortiOS prior to 6.4.13, 7.0.12, and 7.2.5 that does not support BIOS-level signature and file integrity check during bootup, the following steps should be taken if the BIOS version of the FortiGate matches the following versions:

- 6000100 or greater
- 5000100 or greater

To downgrade or upgrade to or from a version that does not support BIOS-level signature and file integrity check during bootup:

1. If the current security level is 2, change the security level to 0. This issue does not affect security level 1 or below.
2. Downgrade to the desired FortiOS firmware version.
3. If upgrading back to 6.4.13, 7.0.12, 7.2.5, 7.4.0, or later, ensure that the security level is set to 0.

4. Upgrade to the desired FortiOS firmware version.
5. Change the security level back to 2.

To verify the BIOS version:

The BIOS version is displayed during bootup:

```
Please stand by while rebooting the system.
Restarting system
FortiGate-1001F (13:13-05.16.2023)
Ver:06000100
```

To verify the security level:

```
# get system status
Version: FortiGate-VM64 v7.4.2,build2571,231219 (GA.F)
First GA patch build date: 230509
Security Level: 1
```

To change the security level:

1. Connect to the console port of the FortiGate.
2. Reboot the FortiGate (`execute reboot`) and enter the BIOS menu.
3. Press [`I`] to enter the *System Information* menu
4. Press [`U`] to enter the *Set security level* menu
5. Enter the required security level.
6. Continue to boot the device.

GUI firmware upgrade does not follow the recommended upgrade path

When performing a firmware upgrade that requires multiple version jumps, the Follow upgrade path option in the GUI does not respect the recommended upgrade path, and instead upgrades the firmware directly to the final version. This can result in unexpected configuration loss. To upgrade a device in the GUI, upgrade to each interim version in the upgrade path individually.

For example, when upgrading from 7.0.7 to 7.0.12 the recommended upgrade path is 7.0.7 -> 7.0.9 -> 7.0.11 -> 7.0.12. To ensure that there is no configuration loss, first upgrade to 7.0.9, then 7.0.11, and then 7.0.12.

Upgrading from 7.0.11 or earlier versions

Upgrading directly from 7.0.11 or earlier versions to 7.0.15 is not supported.

To upgrade:

1. Check the recommended upgrade path using the Upgrade Path Tool.
2. If upgrading from the GUI, upgrade to each firmware version in the upgrade path using the direct upgrade option. See limitations on GUI firmware upgrade does not follow the recommended upgrade path on page 26.

In the event the system hangs due to following an unsupported upgrade path to version 7.0.15, boot up the backup partition from the BIOS, and follow the instructions above to upgrade again.

Product integration and support

The following table lists FortiOS 7.0.16 product integration and support information:

Web browsers	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. 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 0318 and later (needed for FSSO agent support OU in group filters) • Windows Server 2022 Standard • Windows Server 2022 Datacenter • 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	• 6.00302
IPS Engine	• 7.00187

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 113 Google Chrome version 113
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 113
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 113
macOS Ventura 13	Apple Safari version 15 Mozilla Firefox version 113 Google Chrome version 113
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 7.0.16. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
948371	Scanunit should no longer submit known infected files to FortiSandbox.

Data Leak Prevention

Bug ID	Description
977334	Users cannot download files more than 5MB in size using FPX when SSL deep inspection and DLP profiles are enabled.

DNS Filter

Bug ID	Description
1010464	When the DNS filter is enabled with `external-ip-blocklist`, the IPS Engine remains in D status for an extended period of time and the DNS session ends.
1026058	When IP is not resolved or does not exist, the DNS alters the response for the domain and results in a performance issue on the client device.

Explicit Proxy

Bug ID	Description
882867	Proxy policy match resolves IP to multiple internet service application IDs.
1014477	Files do not get uploaded on webmail applications with antivirus, app control, or IPS enabled on an explicit proxy policy.

Firewall

Bug ID	Description
935034	The clock skew tolerance is not reflected.
970179	Unrelated route changes will cause the existing session to be marked dirty.
985508	When `allow-traffic-redirect` is enabled, redirect traffic that ingresses and egresses from the same interface may incorrectly get dropped if the source address of the incoming packet is different from the FortiGate's interface subnet and there is no firewall policy to allow the matched traffic.
1016547	When FortiGate forwards M/C packets to an interface with `egress-shaping-profile` enabled, an interruption occurs in the kernel.

HA

Bug ID	Description
974749	TCP/SCTP sessions count mismatch in an HA pair in A-P mode.
1017177	A WAD processing issue causes the SNMP to not respond in an HA cluster.
1018937	In a FortiGate HA configuration, the tunnel connection to FortiManager is disrupted due to a mismatched serial number and local certificate issue.
1020982	The `hasync` process encounters a CPU usage issue caused by frequent attempts to get the FIB for a deleted vdom.

Intrusion Prevention

Bug ID	Description
1000223	HTTPS connections to a Virtual IP (VIP) on TCP port 8015 are incorrectly blocked by the firewall, displaying an IPS block page even when no packet from the outside to TCP port 8015 should reach the internal VIP address.

IPsec VPN

Bug ID	Description
923150	Some static tunnels in multiple VDOM HA setups do not come up after a firmware upgrade or

Bug ID	Description
	restoring the configuration.
950445	After a third-party router failover, traffic traversing the IPsec tunnel is lost.
1001602	Using IPSec over back to back EMAC VLAN interfaces does not work as expected with NPU offload enabled.
1003830	IPsec VPN tunnel phase 2 instability after upgrading to 7.4.2 on the NP6xlite platform.
1009332	Traffic is interrupted on SPOKEs after upgrading to version 7.0.14 due to one NPU SA race condition.
1042324	The Phase1 monitor BGP remains active when the tunnel is DOWN.

Log & Report

Bug ID	Description
872493	Disk logging files are cached in the kernel, causing high memory usage.
993476	FortiGate encounters a CPU usage issue after rebooting with multiple VDOMs configured.
1005171	After upgrading to version 7.0.14, the system event log generates false positives for individual ports that are not used in any configuration.

Proxy

Bug ID	Description
837568	Restricted SaaS access does not work as expected when `config ssl inspect-all` is enabled.
871273	When the kernel API tries to access the command buffer, the device enters D state due to a kernel interruption.
922093	CPU usage issue in WAD caused by source port exhaustion when using WAN optimization.
933502	When a forward server with proxy authorization is configured with certain traffic, a memory usage issue in the WAD process interrupts the operation of FortiGate.
949464	On FortiGate, a memory usage issue in the WAD process may cause the unit to enter into conserve mode.
979361	After an upgrade, FortiOS encounters an error condition in the application daemon wad caused by an SSL cache error.
982553	After upgrading from version 6.4.13 to version 7.0.12 or 7.0.13, FortiGate experiences a memory usage issue.
1003481	FortiGate may not work as expected due to an error condition in the daemon WAD.

Bug ID	Description
1039006	Some websites cannot open subpages when the HTTP2 header value exceeds 16MB.
1048296	FortiGate experiences an HTTP2 framing error when accessing websites using proxy mode with deep inspection configured due to a frame sizing issue in the WAD process.

REST API

Bug ID	Description
859680	In an HA setup with vCluster, a CMDB API request to the primary cluster does not synchronize the configuration to the secondary cluster.

Routing

Bug ID	Description
852498	BGP packets are marked with DSCP CS0 instead of CS6.
900770	DHCP relay fails after a period of time with SD-WAN.
932092	API call returns recursive next-hop for the gateway address.
978683	The `link-down-failover` command does not bring the BGP peering down when the IPsec tunnel is brought down on the peer FortiGate.
989012	The `ICMP_TIME_EXCEEDED` packet does not follow the original ICMP path displays the incorrect traceroute from the user.
1031394	On the *Network > Routing Objects* page, the *Set AS path* on the *Edit Rule* pane does not allow the use of the full range AS numbers.

SSL VPN

Bug ID	Description
999378	When the GUI tries to write a QR code for the SSL VPN configuration to the file system to send in an email, it tries to write it in a read-only folder.
1003672	When RDP is accessed through SSL VPN web mode, keyboard strokes on-screen lag behind what is being typed by users.
1004633	FortiGate does not respond to ARP packets related to SSL VPN client IP addresses.

Bug ID	Description
1018928	A CPU usage issue occurs in the tvc daemon when the vpn server cannot be reached.
1024837	OneLogin SAML does not work with SSL VPN after upgrading to version 7.0.15 or 7.4.3.
1048915	The SSL VPN web mode flag is determined incorrectly causing the authenticated `POST` request to be dropped.
1061165	SSL VPN encounters a signal 11 interruption and does not work as expected due to a word-length heap memory issue.

System

Bug ID	Description
820268	VIP traffic access to the EMAC VLAN interface uses incorrect MAC address on NP7 platform.
846399	Add 100G speed option for FG-180xF for ports 37, 38, 39, and 40. Upon firmware upgrade, existing port speed configurations are preserved.
863542	FortiGate devices configured behind a proxy may not connect to the FortiToken Mobile server, leading to errors when provisioning tokens.
872391	The session output of `dia sys npu-session list` shows wrong duration when the session is very long (+40 hours).
885057	Add 100G speed option on the FortiGate 1800F.
901721	In a certain edge case, traffic directed towards a VLAN interface could cause a kernel interruption.
907752	On FortiGate 1000D models, the SFP 1G port randomly experiences flapping during operation.
915585	Optimize memory usage, which causes the SLAB memory to increase, in kernel 4.19.
917827	Delay sending LACPDU in kernel 4.19.
920320, 1029447	FortiGate encounters increasing `Rx_CRC_Errors` on SFP ports on the NP6 platform when an Ethernet frame contains carrier extension symbols to Cisco devices.
931604	The FortiGate checksum changes and the FortiManager Backup Mode device status becomes out-of-sync.
932002	Possible infinite loop can cause FortiOS to become unresponsive until the FortiGate goes through a power cycle.
939935	High CPU usage caused by DHCP packets.
943615	When cmdbsvr receives a request to update the version number, it also receives a copy of the query, but this copy is not freed.
947398	When an EMAC VLAN interface is set up on top of a redundant interface, the kernel may encounter an error when rebooting.

Bug ID	Description
954529	The `diagnose npu sniffer stop` command can lead to a traffic outage.
957135	EMAC VLAN interface uses two MAC addresses when it should only use an internally generated MAC address.
957846	High CPU usage caused by DHCP packets.
981433	The ipmcsensord does not work as expected when executing sensor-related commands before the high-end device sensor finishes booting up.
991925	The EMAC VLAN, with a vlanid over a physical interface and a VIP configuration, has the incorrect mac address once traffic is offloaded.
995442	FortiGate may generate a *Power Redundancy Alarm* error when there is no power loss. The error also does not show up in the system log.
999816	FortiGate 100 models may become unresponsive and prevent access to the GUI, requiring a reboot to regain access due to an issue with the SOC3.
1001133	After an upgrade, FortiGate receives a `PSU RPS LOST` traps error despite not having any RPS connected.
1001601	A kernel interruption on FortiGate prevents it from rebooting after an upgrade with a specific configuration.
1003026	On SoC3/SoC4 platforms, a kernel interruption may occur when running WAD monitoring scripts.
1004231	FortiGate loses connections to FortiManager due to a fatal unknown CA after upgrading from version 7.0.13 to 7.0.14.
1018843	When FortiGate experiences a memory usage issue and enters into conserve mode, the system file integrity check may not work as expected and cause the device to shutdown.
1025114	Insufficient free memory on entry-level Fortigate devices with 2 GB RAM may cause unexpected behavior in the IPS engine.
1033589	In a policy-based NGFW, when configuring the FSSO Agent on Windows AD External Connector, traffic is not forwarded.
1037075	On FortiGate, an interruption occurs in the kernel when running WAD process monitoring scripts.
1037393	FortiGate reboots due to the maximum buffer length difference between nTurbo and NPU HW. NPU will fragment packets which are more than 10000, but carries wrong extend info to nTurbo in the 2nd fragment.
1041457	The kernel 4.19 cannot concurrently reassemble IPv4 fragments for a source IP with more than 64 destination IP addresses.
1043205	After upgrading to 7.0.12, the FortiGate to FortiManager tunnel with a load balancer in between no longer operates as expected.
1069554	Upgrading directly from 7.2.4 or earlier versions to 7.2.9, or directly from 7.0.11 or earlier to 7.2.9 is not supported. Users must upgrade following the recommended upgrade path to avoid system hanging.

Upgrade

Bug ID	Description
925567	When upgrading multiple firmware versions in the GUI, the *Follow upgrade path* option does not respect the recommended upgrade path.

VM

Bug ID	Description
909368	If Azure accelerated networking is enabled, IPsec traffic cannot be redistributed using round-robin. This results in a CPU usage issue.
1006570	VPN tunnels go down due to IKE authentication loss after a firmware upgrade on the VM.
1046696	A FortiGate VM HA in Azure Cloud may intermittently go out of synchronization due to an issue in the daemon process.
1054244	FortiToken does not work as expected after moving a FortiGate-VM license to a new VM with the same serial number.
1073016	The OCI SDN connector cannot call the API to the Oracle service when an IAM role is enabled.

VoIP

Bug ID	Description
1004894	VOIPD experiences high memory usage and enters into conserve mode.

Web Filter

Bug ID	Description
1002266	Web filtering does not update rating servers if there is a FortiGuard DNS change.

WiFi Controller

Bug ID	Description
985265	HA setup hostapd issue during stress test.
989929	An kernel interruption occurs on FWF-40F/60F models when WiFi stations connect to SSID on the local radio.
1001672	FortiWiFi reboots or becomes unresponsive when connecting to SSID after upgrading to 7.0.14.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
858921	FortiOS 7.0.16 is no longer vulnerable to the following CVE Reference: • CVE-2023-26207

Known issues

Known issues are organized into the following categories:

- New known issues on page 39
- Existing known issues on page 39

To inquire about a particular bug or report a bug, please contact Customer Service & Support.

New known issues

There are currently no new issues that have been identified in version 7.0.16.

Hyperscale

Bug ID	Description
845269	When editing a Hyperscale firewall policy with an overload CGN IP Pool, the GUI disables endpoint independent filtering `cgn-eif` regardless if it is enabled or not.
895951	The output of the `diagnose sys npu-session stat` command incorrectly shows a `setup rate` of `0` for EIF sessions.
993343	In a Hyperscale VDOM, an interruption in the kernel occurs with `set nat46-generate-ipv6-fragment-header` enabled.
1024902	After FTP traffic passes, the `npu-session stat` does not display the accurate amount of actual sessions on FortiGate.

VM

Bug ID	Description
1082304	FortiGate VMs for ARM64 KVM, AWS, OCI, and for VM64 OPC, encounter an error condition in the kernel when performing an upgrade from version 7.0.15 to 7.0.16. The OCI baremetal kernel image is not supported in version 7.0.16 during an upgrade from versions 7.0.13, 7.0.14, or 7.0.15.

Existing known issues

The following issues have been identified in a previous version of FortiOS and remain in FortiOS7.0.16.

Firewall

Bug ID	Description

843554	If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI.
	This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.
	Workaround: create a new service in the CLI, or move a non-IP type services to the top of the firewall service list. For example, if `ALL` is the first firewall service in the list:
	`config firewall service custom`
	`    edit "unused"`
	`        set tcp-portrange 1`
	`    next`
	`    move "unused" before "ALL"`
	`end`

912740	On a FortiGate managed by FortiManager, after upgrading to 7.0.13, the *Firewall Policy* list may show separate sequence grouping for each policy because the `global-label` is updated to be unique for each policy. **Workaround**: drag and drop the policy to the correct sequence group in the GUI, or remove the `global-label` for each member policy in the group except for the leading policy. • Policy 1 (`global-label "group1"`) • Policy 2 • Policy 3 (`global-label "group2"`) • Policy 4
951984	For local out DNAT traffic, the best output route may not be found.

FortiView

Bug ID	Description
941521	On the *Dashboard > FortiView Websites* page, the *Category* filter does not work in the Japanese GUI.

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.

Bug ID	Description
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.
755177	When upgrading firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
810225	An *undefined* error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
853352	On the *View/Edit Entries* slide-out pane (*Policy & Objects* > *Internet Service Database* dialog), users cannot scroll down to the end if there are over 100000 entries.
881678	On the *Network* > *Routing Objects* page, editing a prefix list with a large number of rule entries fails with an error notification that *The integer value is not within valid range*. **Workaround**: edit a prefix list with a large number of rule entries in the CLI.
898902	In the *System* > *Administrators* dialog, when there are a lot of VDOMs (over 200), the dialog can take more than one minute to load the *Two-factor Authentication* toggle. This issue does not affect configuring other settings in the dialog. **Workaround**: use the CLI to configure `two-factor-authentication` under `config system admin`.
974988	FortiGate GUI should not show a license expired notification due to an expired device-level FortiManager Cloud license if it still has a valid account-level FortiManager Cloud license (function is not affected).

Hyperscale

Bug ID	Description
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.

Bug ID	Description
836976	Sessions being processed by hyperscale firewall policies with hardware logging may be dropped when dynamically changing the `log-processor` setting from `hardware` to `host` for the hardware log sever added to the hyperscale firewall policy. To avoid dropping sessions, change the `log-processor` setting during quiet periods.
838654	Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic.
842659	`srcaddr-negate` and `dstaddr-negate` are not working properly for IPv6 traffic with FTS.
843132	Access control list (ACL) policies added to a hyperscale firewall VDOM that is processing traffic may take longer than expected to become effective. During a transition period, traffic that should be blocked by the new ACL policy will be allowed.
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.
844421	The `diagnose firewall ippool list` command does not show the correct output for overload type IP pools.
846520	NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover.
941784	Hardware session synchronization does not work on FG-480xF devices in hyperscale.
986656	On the HA primary unit, the npu-session list shows many sessions, but the npu-session state shows `0`.

IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.
945367	Disabling `src-check` (RPF) on the parent tunnel is not inherited by ADVPN shortcuts.

Log & Report

Bug ID	Description
850642	Logs are not seen for traffic passing through the firewall caused by numerous simultaneous configuration changes.

Proxy

Bug ID	Description
1001497	FortiGate may enter conserve mode when posting a non or invalid HTTP date through web proxy.

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.
862424	On a FortiGate that has large tables (over 1000 firewall policies, address, or other tables), security rating reports may cause the FortiGate to go into conserve mode.

System

Bug ID	Description
847664	Console may display `mce: [Hardware Error]` error message after fresh image burn or reboot.
861962	When configuring an 802.3ad aggregate interface with a 1 Gbps speed, the port's LED is off and traffic cannot pass through. Affected platforms: 110xE, 220xE, 330xE, 340xE, and 360xE.
934708	The cmdbsvr could not secure the var_zone lock due to another process holding it indefinitely.
935158	The FortiGate console prints `check_gui_redir_file: No such file or directory` after rebooting.

VM

Bug ID	Description
800935	ESXi VLAN interface based on LACP does not work.

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
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the *Managed FortiAPs* page and *FortiAP Status* widget can take a long time to load. This issue does not impact FortiAP operation.
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP devices (over 50). This issue does not impact FortiAP management and operation.
1004338	After an upgrade or reboot on the NP7 platform, WiFi data cannot pass through when the SSID VLAN interface uses the DHCP Relay Server.

ZTNA

Bug ID	Description
819987	SMB drive mapping made through a ZTNA access proxy is inaccessible after rebooting.
848222	ZTNA TCP forwarding is not working when a real server is configured with an FQDN address type. An FQDN address type that can resolve public IPs is not recommended for ZTNA TCP forwarding on real servers because the defined internal DNS database zone is trying to override it at the same time. By doing so, the internal private address may not take effect after rebooting, and causes a ZTNA TCP forwarding failure due to the real server not being found.

Built-in AV Engine

AV Engine 6.00302 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

Built-in IPS Engine

IPS Engine 7.00187 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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

FORTINET®

www.fortinet.com