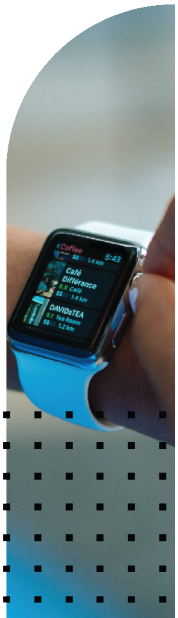
Release Notes

FortiOS 7.0.14



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

February 8, 2024
FortiOS 7.0.14 Release Notes
01-7014-986084-20240208

TABLE OF CONTENTS

Change Log **5**
Introduction and supported models **6**
Supported models 6
Special branch supported models 6
Special notices **8**
Azure-On-Demand image 8
GCP-On-Demand image 8
ALI-On-Demand image 8
Unsupported websites in SSL VPN web mode 9
RDP and VNC clipboard toolbox in SSL VPN web mode 9
CAPWAP offloading compatibility of FortiGate NP7 platforms 9
IP pools and VIPs are now considered local addresses 9
FEC feature design change 10
Hyperscale incompatibilities and limitations 10
SMB drive mapping with ZTNA access proxy 10
New features or enhancements **11**
Upgrade information **12**
Fortinet Security Fabric upgrade 12
Downgrading to previous firmware versions 13
Firmware image checksums 14
IPsec interface MTU value 14
HA role wording changes 14
Strong cryptographic cipher requirements for FortiAP 14
How VoIP profile settings determine the firewall policy inspection mode 15
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 16
Add interface for NAT46 and NAT64 to simplify policy and routing configurations 16
Upgrading 16
Creating new policies 17
Example configurations 17
ZTNA configurations and firewall policies 19
Default DNS server update 20
VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name 20
Product integration and support **21**
Virtualization environments 22
Language support 22
SSL VPN support 23
SSL VPN web mode 23
Resolved issues **24**
Application Control 24

DNS Filter 24
Explicit Proxy 24
Firewall 24
GUI 25
HA 25
Hyperscale 26
Intrusion Prevention 26
IPsec VPN 26
Log & Report 27
Proxy 27
Routing 27
Security Fabric 28
SSL VPN 28
Switch Controller 28
System 29
User & Authentication 30
VM 30
WAN Optimization 30
Web Filter 30
WiFi Controller 31
Common Vulnerabilities and Exposures 31
Known issues 32
Endpoint Control 32
Firewall 32
FortiView 33
GUI 33
HA 34
Hyperscale 34
IPsec VPN 35
Log & Report 35
Security Fabric 35
System 35
User & Authentication 36
VM 36
Web Filter 36
WiFi Controller 36
ZTNA 36
Built-in AV Engine 38
Built-in IPS Engine 39
Limitations 40
Citrix XenServer limitations 40
Open source XenServer limitations 40

Change Log

Date	Change Description
2024-02-07	Initial release.
2024-02-08	Updated Fortinet Security Fabric upgrade on page 12 and Resolved issues on page 24. Added Built-in AV Engine on page 38.

Introduction and supported models

This guide provides release information for FortiOS 7.0.14 build 0601.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.14 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 7.0.14. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0601.

FG-80F-DSL	is released on build 7173.
FG-900G	is released on build 7163.

FG-901G	is released on build 7163.
FG-1000F	is released on build 7164.
FG-1001F	is released on build 7164.
FG-3200F	is released on build 7176.
FG-3201F	is released on build 7176.
FG-3700F	is released on build 7176.
FG-3701F	is released on build 7176.
FG-4800F	is released on build 7176.
FG-4801F	is released on build 7176.
FGR-70F	is released on build 7175.
FGR-70F-3G4G	is released on build 7175.
FWF-80F-2R-3G4G-DSL	is released on build 7173.
FWF-81F-2R-3G4G-DSL	is released on build 7173.

Special notices

- Azure-On-Demand image on page 8
- GCP-On-Demand image on page 8
- ALI-On-Demand image on page 8
- Unsupported websites in SSL VPN web mode on page 9
- RDP and VNC clipboard toolbox in SSL VPN web mode on page 9
- CAPWAP offloading compatibility of FortiGate NP7 platforms on page 9
- IP pools and VIPs are now considered local addresses on page 9
- FEC feature design change on page 10
- Hyperscale incompatibilities and limitations on page 10
- SMB drive mapping with ZTNA access proxy on page 10

Azure-On-Demand image

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

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

GCP-On-Demand image

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

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

ALI-On-Demand image

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

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

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 7.0.14 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.

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.

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

FortiAnalyzer	• 7.0.11
FortiManager	• 7.0.11
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 14
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 7.0.14. When Security Fabric is enabled in FortiOS 7.0.14, all FortiGate devices must be running FortiOS 7.0.14.

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.

Product integration and support

The following table lists FortiOS 7.0.14 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 0314 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	• 6.00295
IPS Engine	• 7.00180

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

Application Control

Bug ID	Description
820481	For firewall policies using inspection-mode proxy, some HTTP/2 sessions may be invalidly detected as unknown application.

DNS Filter

Bug ID	Description
907365	DNS proxy caches DNS responses with only one CNAME record.

Explicit Proxy

Bug ID	Description
901627	Explicit proxy and SD-WAN issue occurs.
942612	Web proxy forward server does not convert HTTP version to the original version when sending them back to the client.
978473	Explicit proxy policy function issues when matching external-threat feed categories.

Firewall

Bug ID	Description
898938	NAT64 does not recover when the interface changes.
953907	Virtual wire pair interface drops all packet if the `prp-port-in`/`prp-port-out` setting is configured under `system npu-setting prp` on FG-101F.

Bug ID	Description
977641	In transparent mode, multicast packets are not forwarded through the bridge and are dropped.

GUI

Bug ID	Description
848660	Read-only administrator may encounter a *Maximum number of monitored interfaces reached* error when viewing an interface bandwidth widget for an interface that does not have the monitor bandwidth feature enabled.
867802	GUI always displays *Access denied* error after logging in.
874502	A prompt to *Login as ReadOnly/ReadWrite* is not displayed when `post-login-banner` is enabled on a FortiGate managed by FortiManager.
969101	Managed FortiAP-s page is not loading for non super-admin users.

HA

Bug ID	Description
871636	HA configuration synchronization packets (Ethertype 0x8893) are dropped when going through VXLAN.
904117	When walking through the session list to change the `ha_id`, some dead sessions could be freed one more time.
924671	There is no response on `ha-mgmt-interfaces` after a reboot when using a VLAN interface based on hd-sw as the ha-mgmt interface.
937246	An error condition occurred while forwarding over a VRRP address, caused by the creation of a new VLAN.
949352	The user.radius checksum is the same in both HA units, but the GUI shows a different checksum on the secondary and the HA status is out of sync.
962681	In a three member A-P cluster, the dhcp lease list (`execute dhcp lease-list`) might be empty on secondary units.

Hyperscale

Bug ID	Description
839958	`service-negate` does not work as expected in a hyperscale deny policy.
940511	In some cases, carrier-grade NAT is dropping traffic.
984852	The HA/AUX ports are not enabled on boot up when using the NPU path option

Intrusion Prevention

Bug ID	Description
923393	IPS logs show incorrect source and destination IP addresses and policy IDs, and the ports are zeros.

IPsec VPN

Bug ID	Description
897867	IPsec VPN between two FortiGates (100F and 60F) experiences slow throughput compared to the available underlay bandwidth.
898961	`diagnose traffictest` issues with dynamic IP addresses and loopback interfaces.
914418	File transfer stops after a while when offloading is enabled.
921691	In FGSP, IKE routes are not removed from the kernel when `secondary-add-ipsec-routes` is disabled.
926002	Incorrect traffic order in IPsec aggregate redundant member list after upgrade.
945873	Inconsistency of `mode-cfg` between phase 1 assigned IP address and destination selector addition.
950012	IPsec tunnels stuck on NP6XLite spoke drop the ESP packet.
950445	After a third-party router failover, traffic traversing the IPsec tunnel is lost.
961305	FortiGate is sending ESP packets with source MAC address of port1 HA virtual MAC address.
968218	When the IPsec tunnel destination MAC address is changed, tunnel traffic may stop.

Log & Report

Bug ID	Description
940814	Administrators without read permissions for the threat weight feature cannot see the event log menu.
954565	Although there is enough disk space for logging, IPS archive full message is shown.
965247	FortiGate syslog format in reliable transport mode is not compliant with RFC 6587.
967692	The received traffic counter is not increasing when the traffic is HTTPS with webfilter.
987261	In the webfilter content block UTM log in proxy inspection mode, `sentbyte` and `rcvdbyte` are zero.

Proxy

Bug ID	Description
790426	An error case occurs in WAD while redirecting the web filter HTTPS sessions.
806556	Unexpected behavior in WAD when the ALPN is set to `http2` in the `ssl-ssh-profile`.
828917, 919781	Unexpected behavior in WAD when there are multiple LDAP servers configured on the FortiGate.
845361	When a client opens two files and sends a compounded request to read and close file A, this causes file B to be closed twice and WAD to crash.
940149	Inadvertent traffic disruption caused by WAD when it receives an HTTP2 data frame payload on a dead stream.
947814	Too many redirects on TWPP after the second KRB keytab is configured.
954104	An error case occurs in WAD when WAD gets the external authenticated users from other daemons.

Routing

Bug ID	Description
781483	Incorrect BGP Originator_ID from route reflector seen on receiving spokes.
890954	The change of an IPv6 route does not mark sessions as dirty nor trigger a route change.
897666	Issue with SD-WAN rule for FortiGuard.

Bug ID	Description
914815	FortiGate 40F-3G4G not adding LTE dynamic route to route table.
926525	`Routing information changed` log is being generated from secondary in an HA cluster.
952908	Locally originated type 5 and 7 LSAs' forward address value is incorrect.
954100	Packet loss status in SD-WAN health check occur after an HA failover.

Security Fabric

Bug ID	Description
782518	Threat feeds are showing that the connection status has not started when it should be connected.
841364	Cisco APIC SDN update times out on large datasets.
956423	In HA, the primary unit may sometimes show a blank GUI screen.

SSL VPN

Bug ID	Description
894704	FortiOS check would block iOS and Android mobile devices from connecting to the SSL VPN tunnel.
898889	The internal website does not load completely with SSL VPN web mode.
906756	Update SSL VPN host check logic for unsupported OS.
957406	OS checklist for SSL VPN in FortiOS does not include macOS Sonoma 14.

Switch Controller

Bug ID	Description
816790	Console printed DSL related error messages when disconnecting the managed FortiSwitch and connecting to the FortiGate again.
858749	Redirected traffic should not hit the firewall policy when `allow-traffic-redirect` is enabled.
911232	Security rating shows an incorrect warning for unregistered FortiSwitches on the *WiFi & Switch Controller > Managed FortiSwitches*.
937065	An exported FortiSwitch port is not correctly showing up/down status.

System

Bug ID	Description
631046	`diagnose sys logdisk smart` does not work for NVMe disk models.
733096	FG-100F HA secondary's unused ports flaps from down to up, then to down.
763739	On FG-200F, the *Outbound* bandwidth in the *Bandwidth* widget does not match outbandwidth setting.
861661	SNMP OID 1.3.6.1.2.1.4.32 ipAddressPrefixTable is not available.
882187	FortiGate enters conserve mode in a few hours after enabling UTM on the policies.
888655	FortiGate queries system DNS for A <Root> and AAAA <Root> servers.
894045	Sensor information widget continuously loading.
909225	ISP traffic is failing with the LAG interfaces on upstream switches.
910700	Ports are flapping and down on the FortiGate 3980E.
912092	FortiGate does not send ARP probe for UDP NP-offloaded sessions.
916493	Fail detection function does not work properly on X1 and X2 10G ports.
919901	For FIPS-CC mode, the strict check for basic constraints should be removed for end entity certificates.
926817	Review the temperature sensor for the SoC4 system.
929904	When L3 or L4 hashing algorithm is used, traffic is not forwarded over the same aggregate member after being offloaded by NP7.
937982	High CPU usage might be observed on entry-level FortiGates if the cache size reaches 10% of the system memory.
938174	ARP issue with VXLAN over IPsec and Soft Switch.
938981	The virtual server http-host algorithm is redirecting requests to an unexpected server.
943948	FortiGate as L2TP client is not working with Cisco ASR as L2TP server.
946413	Temperature sensor value missing for FG-180xF, FG-420xF, and FG-440xF platforms.F
947240	FortiGate is not able to resolve ARPs of few hosts due to their ARP replies not reaching the primary FPM.
955074	MSS clamping is not working on VXLAN over IPsec after upgrading.
960707	Egress shaping does not work on NP when applied on the WAN interface.
962153	A port that uses a copper-transceiver does not update the link status in real-time.
963600	SolarWinds unable to negotiate encryption, no matching host key type found.
966761	SNMP OID 1.3.6.1.2.1.4.34.1.5 ipAddressPrefix is not fully implemented.

Bug ID	Description
971404	Session expiration does not get updated for offloaded traffic between a specific host range.
977231	An error condition occurred in fgfm caused by an out-of-band management configuration.

User & Authentication

Bug ID	Description
837185	Automatic certificate name generation is the same for global and VDOM remote certificates, which can cause certificates to exist with the same name.
864703	ACME client fails to work with some CA servers.
868994	FortiGate receives FSSO user in the format of HOSTNAME$.

VM

Bug ID	Description
938382	OpenStack Queens FortiGate VM HA heartbeat on broadcast is not working as expected.
968740	Unexpected behavior in awsd caused by tags with an empty value on AWS instances while adding a new AWS Fabric connector.

WAN Optimization

Bug ID	Description
954541	In WANOpt transparent mode, WAN optimization does not keep the original source address of the packets.

Web Filter

Bug ID	Description
925801	Custom Images are not seen on Web Filter block replacement page for HTTP traffic in flow mode.

Bug ID	Description
982156	The URL local/user category rating result has only one best match category (longest URL pattern match), and other matched local/user categories cannot be chosen even if the category is configured in the profile.

WiFi Controller

Bug ID	Description
874997	Fetching the registration status does not always work.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
959918	FortiOS 7.0.14 is no longer vulnerable to the following CVE Reference: • CVE-2023-38545

Known issues

The following issues have been identified in version 7.0.14. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Endpoint Control

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

Firewall

Bug ID	Description

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

FortiView

Bug ID	Description
941521	On the *FortiView Web Sites* 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.
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.
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 display a license expired notification due to an expired FortiManager Cloud license if it still has a valid account level FortiManager Cloud license (function is not affected).

HA

Bug ID	Description
810286	FGSP local sessions exist after rebooting an HA pair with A-P mode, and the HW SSE/session count is incorrect.

Hyperscale

Bug ID	Description
795853	VDOM ID and IP addresses in the IPL table are incorrect after disabling EIF/EIM.
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.
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.

Log & Report

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

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.

User & Authentication

Bug ID	Description
765184	RADIUS authentication failover between two servers for high availability does not work as expected.

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 (over 50). This issue does not impact FortiAP management and operation.

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.

Bug ID	Description
	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 6.00295 is released as the built-in AV Engine. Refer to the AV Engine Release Notes for information.

Built-in IPS Engine

IPS Engine 7.00176 is released as the built-in IPS Engine. Refer to the IPS Engine Release Notes for information.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

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

Open source XenServer limitations

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

www.fortinet.com