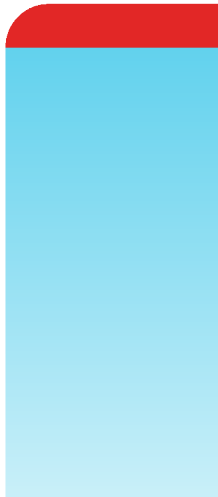


Release Notes

FortiOS 7.0.7



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



August 23, 2024

FortiOS 7.0.7 Release Notes

01-707-848454-20240823

TABLE OF CONTENTS

Change Log	5
Introduction and supported models	7
Supported models	7
Special branch supported models	7
Special notices	9
Azure-On-Demand image	9
GCP-On-Demand image	9
ALI-On-Demand image	9
Unsupported websites in SSL VPN web mode	10
RDP and VNC clipboard toolbox in SSL VPN web mode	10
CAPWAP offloading compatibility of FortiGate NP7 platforms	10
IP pools and VIPs are not considered local addresses for certain FortiOS versions	10
FEC feature design change	11
Support for FortiGates with NP7 processors and hyperscale firewall features	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	15
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	19
VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name	20
GUI firmware upgrade does not respect upgrade path	20
Product integration and support	21
Virtualization environments	21
Language support	22
SSL VPN support	23
SSL VPN web mode	23
Resolved issues	24
Hyperscale	24
Common Vulnerabilities and Exposures	24

Known issues	25
Endpoint Control	25
Explicit Proxy	25
Firewall	25
GUI	26
HA	27
Hyperscale	27
IPsec VPN	28
Proxy	28
Security Fabric	29
SSL VPN	29
System	29
Upgrade	30
User & Authentication	30
Web Filter	30
Built-in AV Engine	31
Built-in IPS Engine	32
Limitations	33
Citrix XenServer limitations	33
Open source XenServer limitations	33

Change Log

Date	Change Description
2022-10-06	Initial release.
2022-10-13	Added <i>Special branch supported models</i> section in Introduction and supported models on page 7 .
2022-10-17	Updated Known issues on page 25 .
2022-10-24	Updated Introduction and supported models on page 7 and Known issues on page 25 .
2022-10-31	Updated Known issues on page 25 .
2022-11-14	Updated Known issues on page 25 .
2022-11-29	Updated Known issues on page 25 .
2022-12-12	Updated Resolved issues on page 24 and Known issues on page 25 .
2022-12-29	Updated Known issues on page 25 .
2023-01-03	Updated Introduction and supported models on page 7 .
2023-01-20	Updated Introduction and supported models on page 7 .
2023-01-27	Updated Known issues on page 25 .
2023-02-02	Updated Product integration and support on page 21 .
2023-02-06	Updated Known issues on page 25 .
2023-02-08	Updated Introduction and supported models on page 7 .
2023-02-14	Updated Known issues on page 25 .
2023-02-17	Updated Introduction and supported models on page 7 .
2023-02-21	Updated Known issues on page 25 .
2023-03-06	Updated Known issues on page 25 .
2023-03-20	Updated Known issues on page 25 .
2023-03-23	Updated Known issues on page 25 . Added VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name on page 20 .
2023-04-04	Updated VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name on page 20 and Known issues on page 25 .
2023-04-17	Updated Known issues on page 25 .
2023-05-02	Updated Known issues on page 25 .

Date	Change Description
2023-05-15	Updated How VoIP profile settings determine the firewall policy inspection mode on page 15 and Known issues on page 25 .
2023-05-29	Updated Known issues on page 25 .
2023-06-13	Updated Known issues on page 25 . Added IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10 .
2023-06-26	Updated Known issues on page 25 .
2023-08-08	Updated Known issues on page 25 .
2023-08-22	Updated Known issues on page 25 .
2023-09-06	Updated Known issues on page 25 , Built-in AV Engine on page 31 , and Built-in IPS Engine on page 32 .
2023-10-04	Updated Known issues on page 25 .
2023-10-17	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10 .
2023-12-13	Updated Known issues on page 25 .
2024-02-13	Updated IP pools and VIPs are not considered local addresses for certain FortiOS versions on page 10 .
2024-03-06	Updated Known issues on page 25 .
2024-04-01	Added GUI firmware upgrade does not respect upgrade path on page 20 .
2024-04-30	Updated Known issues on page 25 .
2024-05-15	Updated Known issues on page 25 .
2024-06-25	Updated Known issues on page 25 .
2024-07-10	Updated Known issues on page 25 .
2024-08-07	Updated Known issues on page 25 .
2024-08-23	Updated Known issues on page 25 .

Introduction and supported models

This guide provides release information for FortiOS 7.0.7 build 0367.

For FortiOS documentation, see the [Fortinet Document Library](#).

Supported models

FortiOS 7.0.7 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-ARM64-AWS, FG-ARM64-KVM, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 7.0.7. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0367.

FG-80F-DSL	is released on build 4730.
FG-400F	is released on build 4701.
FG-401F	is released on build 4701.
FG-600F	is released on build 4701.

FG-601F	is released on build 4701.
FG-1000F	is released on build 6333.
FG-1001F	is released on build 6333.
FG-3000F	is released on build 4701.
FG-3001F	is released on build 4701.
FG-3200F	is released on build 6496.
FG-3201F	is released on build 6496.
FG-3700F	is released on build 6334.
FG-3701F	is released on build 6334.
FG-4800F	is released on build 6401.
FG-4801F	is released on build 6401.
FGR-70F	is released on build 6328.
FGR-70F-3G4G	is released on build 6328.

Special notices

- [Azure-On-Demand image on page 9](#)
- [GCP-On-Demand image on page 9](#)
- [ALI-On-Demand image on page 9](#)
- [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 not considered local addresses for certain FortiOS versions on page 10](#)
- [FEC feature design change on page 11](#)
- [Support for FortiGates with NP7 processors and hyperscale firewall features on page 11](#)

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 not considered local addresses for certain FortiOS versions

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

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

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

FEC feature design change

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

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

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

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

Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.0.7 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F). These FortiGates can also be licensed for hyperscale firewall features. Previous versions of FortiOS supported FortiGates with NP7 processors through special branch firmware builds.

For more information, refer to the [Hyperscale Firewall Release Notes](#).

Upgrade information

Supported upgrade path information is available on the [Fortinet Customer Service & Support site](#).

To view supported upgrade path information:

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

Fortinet Security Fabric upgrade

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

FortiAnalyzer	• 7.0.3
FortiManager	• 7.0.3
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP FortiAP-S FortiAP-U FortiAP-W2	• See Strong cryptographic cipher requirements for FortiAP on page 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. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

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



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

Downgrading to previous firmware versions

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

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

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in, 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 "ipsece-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 usrgroup "L2tpusergroup"
end
```

Add a static route after upgrading:

```
config router static
    edit 1
        set dst 210.0.0.0 255.255.255.0
        set device "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
<pre>config firewall vip46 edit "test-vip46-1" set extip 10.1.100.155 set mappedip 2000:172:16:200::55 next end</pre>	<pre>config firewall vip edit "test-vip46-1" set extip 10.1.100.150 set nat44 disable set nat46 enable set extintf "port24" set ipv6-mappedip 2000:172:16:200::55 next end</pre>

ippool6 object:

Old configuration	New configuration
<pre>config firewall ippool6 edit "test-ippool6-1"</pre>	<pre>config firewall ippool6 edit "test-ippool6-1"</pre>

Old configuration	New configuration
<pre> set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 next end </pre>	<pre> set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 set nat46 enable next end </pre>

NAT46 policy:

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

vip64 object

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

ippool object

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

Old configuration	New configuration
<pre> next end </pre>	<pre> set nat64 enable next end </pre>

NAT64 policy:

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

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.

GUI firmware upgrade does not respect 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.

Product integration and support

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

Web browsers	<ul style="list-style-type: none">• Microsoft Edge 94• Mozilla Firefox version 100• Google Chrome version 101 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	<ul style="list-style-type: none">• Microsoft Edge 44• Mozilla Firefox version 74• Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	<ul style="list-style-type: none">• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	<ul style="list-style-type: none">• 5.0 build 0306 and later (needed for FSSO agent support OU in group filters)<ul style="list-style-type: none">• Windows Server 2019 Standard• Windows Server 2019 Datacenter• Windows Server 2019 Core• Windows Server 2016 Datacenter• Windows Server 2016 Standard• Windows Server 2016 Core• Windows Server 2012 Standard• Windows Server 2012 R2 Standard• Windows Server 2012 Core• Windows Server 2008 64-bit (requires Microsoft SHA2 support package)• Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)• Windows Server 2008 Core (requires Microsoft SHA2 support package)• Novell eDirectory 8.8
AV Engine	<ul style="list-style-type: none">• 6.00276
IPS Engine	<ul style="list-style-type: none">• 7.00126

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	<ul style="list-style-type: none"> 8.1 Express Edition, Dec 17, 2019
Linux KVM	<ul style="list-style-type: none"> Ubuntu 18.0.4 LTS Red Hat Enterprise Linux release 8.4 SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	<ul style="list-style-type: none"> 2012R2 with Hyper-V role
Windows Hyper-V Server	<ul style="list-style-type: none"> 2019
Open source XenServer	<ul style="list-style-type: none"> Version 3.4.3 Version 4.1 and later
VMware ESX	<ul style="list-style-type: none"> Versions 4.0 and 4.1
VMware ESXi	<ul style="list-style-type: none"> Versions 6.5, 6.7, and 7.0.

Language support

The following table lists language support information.

Language support

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

SSL VPN support

SSL VPN web mode

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

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 100 Google Chrome version 101
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 100 Google Chrome version 101
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 100 Google Chrome version 101
macOS Monterey 12.4	Apple Safari version 15 Mozilla Firefox version 100 Google Chrome version 101
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

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

Resolved issues

The following issues have been fixed in version 7.0.7. To inquire about a particular bug, please contact [Customer Service & Support](#).

Hyperscale

Bug ID	Description
763966	FGSP synchronizes NP sessions of all VDOMs when syncvd is only set for hyperscale VDOM.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
846234	FortiOS 7.0.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2022-40684
846854	FortiOS 7.0.7 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none">• CVE-2022-40684

Known issues

The following issues have been identified in version 7.0.7. 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.

Explicit Proxy

Bug ID	Description
803228	When converting an explicit proxy session to SSL redirect, traffic may be interrupted inadvertently in some situations.

Firewall

Bug ID	Description
808264	Stress test shows packet loss when testing with flow inspection mode and application control.
860480	FG-3000D cluster kernel panic occurs when upgrading from 7.0.5 to 7.0.6 and later.
861990	Increased CPU usage in softirq after upgrading from 7.0.5 to 7.0.6.

GUI

Bug ID	Description
440197	On the <i>System > FortiGuard</i> page, the override FortiGuard server for <i>AntiVirus & IPS Updates</i> shows an <i>Unknown</i> status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the <i>Network > Interfaces</i> page when VDOM mode is enabled, the <i>Global</i> 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 <i>Policy & Objects > Firewall Policy</i> 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	<i>System > Certificates</i> 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.
719476	FortiLink NAC matched device is displayed in the CLI but not in the GUI under <i>WiFi & Switch Controller > NAC Policies > View Matched Devices</i> .
729406	New IPsec design <code>tunnel-id</code> still displays the gateway as an IP address, when it should be a tunnel ID.
755177	When upgrade firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
777145	<i>Managed FortiSwitches</i> page incorrectly shows a warning about an unregistered FortiSwitch even though it is registered. This only impacts transferred or RMAed FortiSwitches. This is only a display issue with no impact on the FortiSwitch's operation. Workaround: confirm the FortiSwitch registration status in the FortiCare portal.
810225	An <i>undefined</i> error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
831885	Unable to access GUI via HA management interface of secondary unit.
853352	When viewing entries in the slide-out window of the <i>Policy & Objects > Internet Service Database</i> page, users cannot scroll down to the end if there are over 100000 entries.

HA

Bug ID	Description
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.
819872	HA split brain scenario occurs after upgrading from 6.4.6 to 7.0.6, and HA heartbeats are lost followed by a kernel panic. Affected platforms: NP7 models.
823687	A cluster is repeatedly out-of sync due to external files (SSLVPN_AUTH_GROUPS) when there are frequent user logins and logouts.
830463	After shutting down the HA primary unit and then restarting it, the uptime for both nodes is zero, and it fails back to the former primary unit.

Hyperscale

Bug ID	Description
782674	A few tasks are hung on issuing <code>stat verbose</code> on the secondary device.
804742	After changing hyperscale firewall policies, it may take longer than expected for the policy changes to be applied to traffic. The delay occurs because the hyperscale firewall policy engine enhancements added to FortiOS 7.0.6 may cause the FortiGate to take extra time to compile firewall policy changes and generate a new policy set that can be applied to traffic by NP7 processors. The delay is affected by hyperscale policy set complexity, the total number of established sessions to be re-evaluated, and the rate of receiving new sessions.
805846	In the FortiOS MIB files, the trap fields <code>fgFwIppStatsGroupName</code> and <code>fgFwIppStatsInusePBAs</code> have the same OID. As a result, the <code>fgFwIppStatsInusePBAs</code> field always returns a value of 0.
807476	After packets go through host interface TX/RX queues, some packet buffers can still hold references to a VDOM when the host queues are idle. This causes a VDOM delete error with <code>unregister_vf</code> . If more packets go through the same host queues for other VDOMs, the issue should resolve by itself because those buffers holding the VDOM reference can be pushed and get freed and recycled.
810025	Using EIF to support hairpinning does not work for NAT64 sessions.
810379	Creating an access control list (ACL) policy on a FortiGate with NP7 processors causes the <code>npd</code> process to crash.
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.
812833	FortiGate still holds <code>npu-log-server</code> related configuration after removing hyperscale license.
836474	Changes in the zone configuration are not updated by the NPD on hyperscale.

Bug ID	Description
836976	Sessions being processed by hyperscale firewall policies with hardware logging may be dropped when dynamically changing the <code>log-processor</code> setting from <code>hardware</code> to <code>host</code> for the hardware log sever added to the hyperscale firewall policy. To avoid dropping sessions, change the <code>log-processor</code> setting during quiet periods.
838654	Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic.
839958	<code>service-negate</code> does not work as expected in a hyperscale deny policy.
842659	<code>srcaddr-negate</code> and <code>dstaddr-negate</code> are not working properly for IPv6 traffic with FTS.
843197	Output of <code>diagnose sys npu-session list/list-full</code> does not mention policy route information.
843266	Diagnose command should be available to show <code>hit_count/last_used</code> for policy route and NPU session on hyperscale VDOM.
843305	Get <code>PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS</code> console error log when system boots up.
844421	The <code>diagnose firewall ippool list</code> 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.

IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.
763205	IKE crashes after HA failover when the <code>enforce-unique-id</code> option is enabled.
778243	When <code>net-device</code> is enabled on the hub, the tunnel interface IP is missing in the routing table.
810833	IPsec static router gateway IP is set to the gateway of the tunnel interface when it is not specified.
822651	NP dropping packet in the incoming direction for SoC4 models.

Proxy

Bug ID	Description
727629	An error case occurs in WAD while handling the HTTP requests for an explicit proxy policy.
799237	WAD crash occurs when TLS/SSL renegotiation encounters an error.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
794703	Security Rating report for <i>Rogue AP Detection</i> and <i>FortiCare Support</i> checks show incorrect results.
825291	Security rating test for <i>FortiAnalyzer</i> fails when connected to FortiAnalyzer Cloud.

SSL VPN

Bug ID	Description
819754	Multiple DNS suffixes cannot be set for the SSL VPN portal.
852566	User peer feature for one group to match to multiple user peers in the authentication rules is broken.

System

Bug ID	Description
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. Workaround: set the <code>auto-asic-offload</code> option to <code>disable</code> in the firewall policy.
751715	Random LTE modem disconnections due to certain carriers getting unstable due to WWAN modem USB speed under super-speed.
798091	After upgrading from 6.4.9 to 7.0.5, the FG-110xE's 1000M SFP interface may fail to auto-negotiate and cannot be up due to the missed auto-negotiation.
798303	The threshold for conserve mode is lowered.
799570	High memory usage occurs on FG-200F.
810879	DoS policy ID cannot be moved in GUI and CLI when enabling multiple DoS policies.
812957	When setting the <code>speed</code> of 1G SFP ports on FG-180xF platforms to <code>1000full</code> , the interface does not come up after rebooting.
815360	NP7 platforms may encounter a kernel panic when deleting more than two hardware switches at the same time.
830415	FEX-40D-NAM model support was removed after upgrading to 7.0.6 or 7.0.7.

Bug ID	Description
847077	Can't find xitem. Drop the response. error appears for DHCP OFFER packets in the DHCP relay debug.
850430	DHCP relay does not work properly with two DHCP relay servers configured.
882187	FortiGate might enter conserve mode if disk logging is enabled and <code>log-traffic all</code> is set in a policy.
883071	Kernel panic occurs due to null pointer dereference.
1041457	On FortiGate, kernel 4.19 does not work as expected when concurrently reassembling fragmented packets that have more than 64 destination IPv4 addresses.

Upgrade

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

User & Authentication

Bug ID	Description
754725	After updating the FSSO DC agent to version 5.0.0301, the DC agent keeps crashing on Windows 2012 R2 and 2016, which causes lsass.exe to reboot.
825505	<p>After a few days, some devices are not displayed in the <i>Users & Devices > Device Inventory</i> widget and <i>WiFi & Switch Controller > FortiSwitch Ports</i> page's <i>Device Information</i> column due to a mismatch in the device count between the following commands.</p> <ul style="list-style-type: none"> <code>diagnose user device list</code> <code>diagnose user device stats</code> <code>diagnose user-device-store device memory list</code> <p>Workaround: restart the WAD process or reboot the FortiGate to recover the device count for the user device store list.</p>

Web Filter

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

Built-in AV Engine

AV Engine 6.00276 is released as the built-in AV Engine. Refer to the [AV Engine Release Notes](#) for information.

Built-in IPS Engine

IPS Engine 7.00126 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

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.