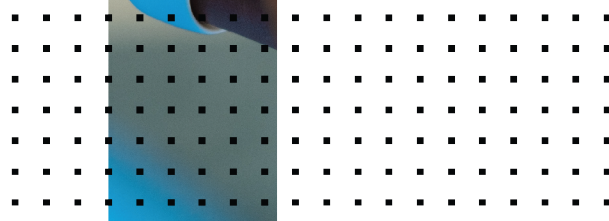
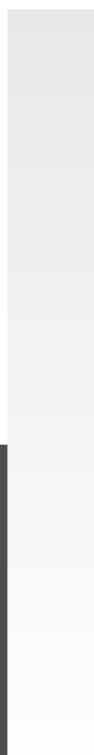
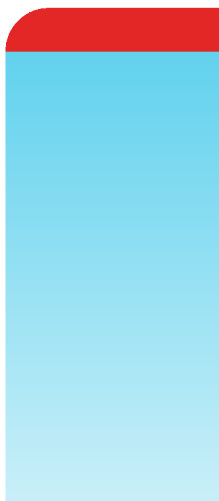


Release Notes

FortiOS 7.0.5



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



February 22, 2022

FortiOS 7.0.5 Release Notes

01-705-779589-20220222

TABLE OF CONTENTS

Change Log	5
Introduction and supported models	6
Supported models	6
Special notices	7
Azure-On-Demand image	7
GCP-On-Demand image	7
ALI-On-Demand image	7
Unsupported websites in SSL VPN web mode	8
RDP and VNC clipboard toolbox in SSL VPN web mode	8
FEC feature design change	8
Upgrade information	9
Fortinet Security Fabric upgrade	9
Downgrading to previous firmware versions	10
Firmware image checksums	11
IPsec interface MTU value	11
HA role wording changes	11
Strong cryptographic cipher requirements for FortiAP	11
How VoIP profile settings determine the firewall policy inspection mode	12
L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1	12
Add interface for NAT46 and NAT64 to simplify policy and routing configurations	12
Upgrading	12
Creating new policies	13
Example configurations	13
ZTNA configurations and firewall policies	15
Default DNS server update	15
Product integration and support	17
Virtualization environments	17
Language support	18
SSL VPN support	19
SSL VPN web mode	19
Resolved issues	20
Anti Virus	20
Proxy	20
System	20
Known issues	21
Endpoint Control	21
Firewall	21
GUI	21
HA	22
IPsec VPN	22

Routing	22
Security Fabric	23
SSL VPN	23
System	23
VM	24
WAN Optimization	24
WiFi Controller	24
Built-in IPS engine	25
Resolved engine issues	25
Limitations	26
Citrix XenServer limitations	26
Open source XenServer limitations	26

Change Log

Date	Change Description
2022-02-09	Initial release.
2022-02-14	Updated Fortinet Security Fabric upgrade on page 9 and Known issues on page 21 .
2022-02-22	Updated Known issues on page 21 . Added Built-in IPS engine on page 25 .

Introduction and supported models

This guide provides release information for FortiOS 7.0.5 build 0304.

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

Supported models

FortiOS 7.0.5 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-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, 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-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special notices

- [Azure-On-Demand image on page 7](#)
- [GCP-On-Demand image on page 7](#)
- [ALI-On-Demand image on page 7](#)
- [Unsupported websites in SSL VPN web mode on page 8](#)
- [RDP and VNC clipboard toolbox in SSL VPN web mode on page 8](#)
- [FEC feature design change on page 8](#)

Azure-On-Demand image

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

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

GCP-On-Demand image

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

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

ALI-On-Demand image

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

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

Unsupported websites in SSL VPN web mode

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

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

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

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.

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

FortiAnalyzer	• 7.0.2
FortiManager	• 7.0.2
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 11
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 7.0.5. When Security Fabric is enabled in FortiOS 7.0.5, all FortiGate devices must be running FortiOS 7.0.5.

Downgrading to previous firmware versions

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

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

Firmware image checksums

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

IPsec interface MTU value

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

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

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

HA role wording changes

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

Strong cryptographic cipher requirements for FortiAP

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

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1 and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE) will support strong ciphers in the future release of version 5.4.3.

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

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

How VoIP profile settings determine the firewall policy inspection mode

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

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

To make L2TP over IPsec work after upgrading:

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

```
config vpn l2tp
  set eip 210.0.0.254
  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 "l2tp.root"
  next
end
```

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

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

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

Upgrading

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

The following CLI commands have been removed:

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

The following GUI pages have been removed:

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

Creating new policies

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

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

Example configurations

`vip46` object:

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

`ippool6` object:

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

NAT46 policy:

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

vip64 object

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

ippool object

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

Old configuration	New configuration
<pre> set startip 172.16.201.155 set endip 172.16.201.155 next end </pre>	<pre> set startip 172.16.201.155 set endip 172.16.201.155 set nat64 enable next end </pre>

NAT64 policy:

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

ZTNA configurations and firewall policies

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

When upgrading from FortiOS 7.0.1 or below:

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

Default DNS server update

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

the default FortiGuard server, upgrading will retain the existing DNS servers and DNS protocol configuration.

Product integration and support

The following table lists FortiOS 7.0.5 product integration and support information:

Web browsers	• Microsoft Edge 94 • Mozilla Firefox version 96 • Google Chrome version 97 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 44 • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
Fortinet Single Sign-On (FSSO)	• 5.0 build 0304 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
AV Engine	• 6.00270
IPS Engine	• 7.00105

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 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 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 96 Google Chrome version 97
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 96 Google Chrome version 97
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 96 Google Chrome version 97
macOS Monterey 12.0	Apple Safari version 15 Mozilla Firefox version 96 Google Chrome version 97
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 7.0.5. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Anti Virus

Bug ID	Description
778298	Traffic is blocked when an AV profile is enabled in proxy inspection mode in an IPsec scenario with NPU offloading enabled.

Proxy

Bug ID	Description
772041	WAD crash at signal 11.
778659	Proxy inspection fails due to <code>ipsapp session open failed: all providers busy</code> .

System

Bug ID	Description
778474	dhcpcd is not processing discover messages if they contain a 0 length option, such as 80 (rapid commit). The warning, <code>length 0 overflows input buffer</code> , is displayed.

Known issues

The following issues have been identified in version 7.0.5. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Endpoint Control

Bug ID	Description
708545	The WAD daemon is triggered to fetch the FortiClient information based on a ZTNA EMS tag enabled for checking in a proxy policy. It is then possible to get a ZTNA EMS tag in the firewall dynamic address and get the expected traffic control.
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. Workaround: delete the EMS Cloud entry then add it back.

Firewall

Bug ID	Description
719311	FortiGate shows partial view of policies after upgrading.

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.

Bug ID	Description
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.
713529	When FortiAnalyzer is configured, the HTTPS daemon may crash while processing some FortiAnalyzer log requests. There is no apparent impact on the GUI operation.
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.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
771389	SNMP community name with one extra character at the end stills matches when HA is enabled.

IPsec VPN

Bug ID	Description
699973	IPsec aggregate shows down status on <i>Interfaces</i> , <i>Firewall Policy</i> , and <i>Static Routes</i> configuration pages.

Routing

Bug ID	Description
745856	The default SD-WAN route for the LTE wwan interface is not created. Workaround: add a random gateway to the wwan member. <pre>config system sdwan config members edit 2 set interface "wwan"</pre>

Bug ID	Description
	<pre>set gateway 10.198.58.58 set priority 100 next end end</pre>

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.

SSL VPN

Bug ID	Description
757450	SNAT is not working in SSL VPN web mode when accessing an SFTP server.

System

Bug ID	Description
644782	A large number of detected devices causes httpsd to consume resources, and causes low-end devices to enter conserve mode.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.
699152	QinQ (802.1ad) support needed on the following models: FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3600E, and FG-3601E.
706543	FortiGuard DDNS does not update the IP address when the PPPoE reconnects.
708228	A DNS proxy crash occurs during <code>ssl_ctx_free</code> .
763185	High CPU usage on platforms with low free memory upon IPS engine initialization.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.

VM

Bug ID	Description
689047	ARM64-KVM has kernel panic.

WAN Optimization

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

WiFi Controller

Bug ID	Description
745642	Consider not generating rogue AP logs once a certain AP has been marked as accepted.
750425	In RADIUS MAC authentication, the FortiGate NAS-IP-Address will revert to 0.0.0.0 after using the FortiGate address.
757189	A batch of APs in cluster are exhibiting control messages that the maximal retransmission limit reached, and the APs disconnect from the FortiGate.
775157	A packet with the wrong IP header could not be processed by the CAPWAP driver, which randomly causes the FortiGate to reboot.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
683066	IPS engine crashes and consumes high CPU.
713508	Low download performance occurs when SSL deep Inspection is enabled on aggregate and VLAN interfaces when nTurbo is enabled.
730235	The IPS engine application crashed during traffic testing (FG-5001E, FG-5001E1).
752466	Deep inspection is causing downloads to fail in an ADVPN environment.
752540	FortiGate keeps outputting warning messages while rebooting.
754216	Flow mode web filter replacement message is not displayed using upstream proxy when using HTTPS.
754579	Application performance is ten times worse when IPS is applied in flow mode.
755223	There is no detection trigger packet in the PCAP.
755294	Firefox gives <code>SEC_ERROR_REUSED_ISSUER_AND_SERIAL</code> error when ECDSA CA is configured for deep inspection.
755851	Mixed mode inspection causing SSL error for pass through proxy traffic.
756398	An invalid character string is inserted in the IPS log sent to the TCP Syslog server.
756616	High CPU usage in proxy-based policy with deep inspection and IPS sensor.
757122	The wildcard strings do not work as expected.
757314	IPS engine crashes after upgrading to 6.4.7 and is affecting traffic.
757951	CIFS oversize files cannot be blocked.
760555	Web filter UTM logged unexpected URLs, such as <code>url="https:///".</code>
765859	Repeated IPS engine signal 11 and signal 7 crashes occur.

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© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.