FortiOS - Release Notes

Version 5.6.4

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 COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdocs@fortinet.com

September 18, 2018
FortiOS 5.6.4 Release Notes
01-564-475635-20180918

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-04-26	Initial release.
2018-04-27	Added IE 11 to *Product Integration and Support* > *FortiOS 5.6.4 support* > *Explicit Web Proxy Browser*. Added FG-90E and FG-91E models to *Introduction* > *Supported models*. Added 416790 to *Resolved Issues*.
2018-04-30	Added 477885 to *Known Issues*. Moved 456566 from *Known Issues* to *Resolved Issues*.
2018-05-03	Added 464101 and 477670 to *Resolved Issues*.
2018-05-22	Updated *Special Notices* > *Built-in certificate*.
2018-05-23	Added 416452 to *Resolved Issues* and updated *Upgrade Information* > *Physical interface inclusion in zones*.
2018-06-01	Removed inapplicable note from *Upgrade Information*.
2018-06-04	Added 486466 to *Known Issues*.
2018-06-07	Updated description for 466314 in *Resolved Issues*.
2018-06-08	Added 479311 to *Known Issues*.
2018-06-18	Deleted 374247, 375036, and 439185 from *Known Issues*.
2018-06-20	Deleted *Upgrade Information* > *FortiGate-VM64-Azure upgrade*.
2018-08-02	Updated 435388 description and moved it from *Resolved Issues* to *Known Issues*.
2018-09-11	Added 476617 to *Known Issues*.
2018-09-18	Updated 476617 in *Known Issues*.

Introduction

This document provides the following information for FortiOS 5.6.4 build 1575:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 5.6.4 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001C, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30D, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-30D-POE, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-SVM, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 5.6.4 images are delivered upon request and are not available on the customer support firmware download page.

Special branch supported models

The following models are released on a special branch of FortiOS 5.6.4. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1575.

FOS-VM64-XEN	is released on build 3270.

VXLAN supported models

The following models support VXLAN.

FortiGate	FG-30E, FG-30E-MI, FG-30E-MN, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-MC, FG-60E-MI, FG-60E-POE, FG-60EV, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-MC, FWF-60E-MI, FWF-60EV, FWF-61E
FortiGate Rugged	FGR-30D, FGR-30D-A, FGR-35D
FortiGate VM	FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-NPU, FG-VM64-OPC, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN

.

Special Notices

Built-in certificate

New FortiGate and FortiWiFi D-series and above are shipped with a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate and FortiWiFi-92D hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result.

FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.4, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

FortiClient profile changes

With introduction of the Fortinet Security Fabric, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

The FortiClient profile on FortiGate is for FortiClient features related to compliance, such as Antivirus, Web Filter, Vulnerability Scan, and Application Firewall. You may set the *Non-Compliance Action* setting to *Block* or *Warn*. FortiClient users can change their features locally to meet the FortiGate compliance criteria. You can also use FortiClient EMS to centrally provision endpoints. The EMS also includes support for additional features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

FortiExtender support

Due to OpenSSL updates, FortiOS 5.6.4 cannot manage FortiExtender 3.2.0 or earlier. If you run FortiOS 5.6.4 with FortiExtender, you must use a newer version of FortiExtender such as 3.2.1 or later.

Using ssh-dss algorithm to log in to FortiGate

In version 5.4.5 and later, using `ssh-dss` algorithm to log in to FortiGate via SSH is no longer supported.

Upgrade Information

Upgrading to FortiOS 5.6.4

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*.

If you are upgrading from version 5.6.2, this caution does not apply.
Before upgrading, ensure that port 4433 is not used for `admin-port` or `admin-sport` (in `config system global`), or for SSL VPN (in `config vpn ssl settings`).
If you are using port 4433, you must change `admin-port`, `admin-sport`, or the SSL VPN port to another port number before upgrading.

After upgrading, if FortiLink mode is enabled, you must manually create an explicit firewall policy to allow RADIUS traffic for 802.1x authentication from the FortiSwitch (such as from the FortiLink interface) to the RADIUS server through the FortiGate.

Physical interface inclusion in zones

Upgrading from 5.6.3 or later removes all of the members of a zone if the zone contains a physical interface and at least one of that physical interface's VLAN interfaces is removed. For example:

Before Upgrade:

```
config system zone
   edit "Trust"
   set interface "port1" "Vlan01" "Vlan02" "Vlan03"
next
```

After Upgrade:

```
config system zone
   edit "Trust"
next
```

Remove "port1" from the list and the upgrade will retain the VLANs.

Conditions when physical zone members are removed:

- If a physical interface has a VLAN associated (regardless of whether they are in the same zone or any zone)

Conditions when VLAN zone members are removed:

- If the parent physical interface is also set on a zone

You can use the following options to prepare for the upgrade:

- Use only physical interfaces that have no VLAN associations

  Or:
- Create new VLANs in place of current physical interface zone members, and remove all physical zone members from zones using only the associated, new VLAN entries.

Security Fabric upgrade

FortiOS 5.6.4 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 5.6.1
- FortiClient 5.6.0
- FortiClient EMS 1.2.2
- FortiAP 5.4.2 and later
- FortiSwitch 3.6.2 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

Before upgrading any product, you must read the *FortiOS Security Fabric Upgrade Guide*.

FortiClient profiles

After upgrading from FortiOS 5.4.0 to 5.4.1 and later, your FortiClient profiles will be changed to remove a number of options that are no longer supported. After upgrading, review your FortiClient profiles to make sure they are configured appropriately for your requirements and either modify them if required or create new ones.

The following FortiClient Profile features are no longer supported by FortiOS 5.4.1 and later:

- Advanced FortiClient profiles (XML configuration).
- Advanced configuration, such as configuring CA certificates, unregister option, FortiManager updates, dashboard Banner, client-based logging when on-net, and Single Sign-on Mobility Agent.
- VPN provisioning.
- Advanced AntiVirus settings, such as Scheduled Scan, Scan with FortiSandbox, and Excluded Paths.

- Client-side web filtering when on-net.
- iOS and Android configuration by using the FortiOS GUI.

With FortiOS 5.6.4, endpoints in the Security Fabric require FortiClient 5.6.0. You can use FortiClient 5.4.3 for VPN (IPsec VPN, or SSL VPN) connections to FortiOS 5.6.2, but not for Security Fabric functions.

It is recommended that you use FortiClient Enterprise Management Server (EMS) for detailed Endpoint deployment and provisioning.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.4, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

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
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles

If you have long VDOM names, you must shorten the long VDOM names (maximum 11 characters) before downgrading:

1. Back up your configuration.
2. In the backup configuration, replace all long VDOM names with its corresponding short VDOM name.
   For example, replace `edit <long_vdom_name>/<short_name>` with `edit <short_name>/<short_name>`.
3. Restore the configuration.
4. Perform the downgrade.

Amazon AWS enhanced networking compatibility issue

With this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.6.4 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover

the downgraded image.

When downgrading from 5.6.4 to older versions, running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

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*.

Product Integration and Support

FortiOS 5.6.4 support

The following table lists 5.6.4 product integration and support information:

Web Browsers	• Microsoft Edge 38 • Mozilla Firefox version 54 • Google Chrome version 59 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 40 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 53 • Google Chrome version 58 • Apple Safari version 10 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Security Fabric upgrade on page 10. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Security Fabric upgrade on page 10. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient Microsoft Windows	See important compatibility information in Security Fabric upgrade on page 10. • 5.6.1 If FortiClient is managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.
FortiClient Mac OS X	See important compatibility information in Security Fabric upgrade on page 10. • 5.6.0 If FortiClient is managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.
FortiClient iOS	• 5.4.3 and later
FortiClient Android and FortiClient VPN Android	• 5.4.1 and later

FortiAP	• 5.4.2 and later • 5.6.0
FortiAP-S	• 5.4.3 and later • 5.6.0
FortiSwitch OS (FortiLink support)	• 3.6.2 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C.
FortiSandbox	• 2.3.3 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0267 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExtender	• 3.2.1 and later See FortiExtender support on page 8.
AV Engine	• 5.247
IPS Engine	• 3.442
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, and 2012 R2
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5  FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

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 standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04	2336. Download from the Fortinet Developer Network https://fndn.fortinet.net.

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

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

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) Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 54 Google Chrome version 59
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.

SSL VPN host compatibility list

It is recommended to verify the accuracy of the GUID for the software you are using for SSL VPN host check. The following Knowledge Base article at http://kb.fortinet.com/ describes how to identify the GUID for antivirus and firewall products: How to add non listed 3rd Party AntiVirus and Firewall product to the FortiGate SSL VPN Host check.

After verifying GUIDs, you can update GUIDs in FortiOS using this command:

```
config vpn ssl web host-check-software
```

Following is an example of how to update the GUID for AVG Internet Security 2017 on Windows 7 and Windows 10 by using the FortiOS CLI.

The GUIDs in this example are only for AVG Internet Security 2017 on Windows 7 and Windows 10. The GUIDs might be different for other versions of the software and other operation systems.

To update GUIDs in FortiOS:

1. Use the `config vpn ssl web host-check-software` command to edit the `AVG-Internet-Security-AV` variable to set the following GUID for AVG Internet Security 2017: `4D41356F-32AD-7C42-C820-63775EE4F413`.
2. Edit the `AVG-Internet-Security-FW` variable to set the following GUID: `757AB44A-78C2-7D1A-E37F-CA42A037B368`.

Resolved Issues

The following issues have been fixed in version 5.6.4. For inquires about a particular bug, please contact Customer Service & Support.

Authentication

Bug ID	Description
456638	Wildcard `remote-admin` logon in browser with customized password gets FortiGate message `....uses default password`.
456719	RADIUS attribute NAS-IP-Address incorrectly decoded.
457883	Certificate warning `SAN` missing in Chrome when redirecting to the HTTPS captive portal even though CA certificate is trusted.
459598	Security flaw on captive portal with L3 authentication on FortiGate.
460229	Existing terminal server sessions overridden with the last TS user that logged in.
460913	High response time when `rsso-flush-ip-session` is enabled.
462204	NTLM authenticaton problem after upgrading from 5.2.8 to 5.6.2.
464186	`authd` does not send back full certificate chain to client after re-signing certificate.
464610	FortiGate sends wrong client MAC address in external captive portal forward URL.
466929	FSSO will failover to secondary servers if an incorrect password is entered.
468686	`cn-match` value is not matching the correct value.
471120	ForitGate clears sessions for all users when RADIUS accounting STOP message is sent for one user.
472972	LDAP search does not return group membership for FSSO local polling users with comma in username.
475052	No following query if `CHKPRIMARYGRP` is not found.

AV

Bug ID	Description
386130	MAPI protocol does not exist in SNMP statistics for proxy.
456704	When signature update runs on FortiGate device, `scanunit` process says busy and drop.

DLP

Bug ID	Description
470412	DLP profile to block banned words with regex does not work on all web sites.

Endpoint Control

Bug ID	Description
439638	Infinite Outlook security pop-ups.

Firewall

Bug ID	Description
398024	SLB SSL offload loading issue with form page.
453920	Central NAT behavior is strange.
459615	Session count is incorrect.
462155	Session clash seen for ICMP traffic from the same source IP.
467025	Can't create the second IPv6 VIP64 which has the same ext/int IP with existing one, but different port-forwarding port.
467382	Cannot create custom categories in VDOMs when using flow-based policy-based mode.
472224	VIP LB health check erroneous status.

FortiGate 80D

Bug ID	Description
416567	Traffic dropped and crashlogs generate the logs: `Interface port1 has a transmit timeout.`

FortiGate 100E

Bug ID	Description
477670	FortiGate 100E stops processing traffic and responding to management on HTTP, HTTPS, SSH, ping, etc.

GUI

Bug ID	Description
416452	Add permission checks for APIs on VIP, Address and Reputation pages

Bug ID	Description
442886	In GTP Profile, some fields in GUI (`Addr Objects`) show spinning wheel and can't be selected.
446756	Guest user print template can’t display pictures while printing.
451098	FortiOS IPS profile filter in GUI not displaying OS signatures correctly.
456566	In firewall policy list, need to add support for custom sections.
459904	Rogue AP Monitor does not show the *Name* of the AP in the *Detected By* column.
464315	GUI error *Failed to save changes* if logged in with super_admin account that starts with special character `.\\`.
464333	Password for *Guest User* created via the *Guest Management* portal is replaced by `ENC XXXX` instead of clear text.
464838	Can't edit *Zone Interface* in GUI if name has a space.
468207	Unable to edit *User Group* when its name contains a space.
468459	Translation issue on *Countries*.

HA

Bug ID	Description
441078	The time duration of packet-transporting process stops to pre-master node after HA failover takes too long.
453884	Filter is not working in case traffic is handled by HA cluster unit without management VDOM (vlcuster).
457554	FortiGate does not send syslog after `ha-mgmt-interface` link goes down and then up.
457877	Packets dropped with TNS session-helper enabled on FGSP cluster.
460396	FG-201E cluster out of sync due to mismatch in switch controller config between master and slave.
461589	HA checksum keeps changing after each reboot.
461915	When *standalone config sync* is enabled in FGSP, IPv6 setting of interface is sync’ed.
462021	Update daemon runs in slave unit after upgrading.
466379	After HA failover, new master unit use an OSPF MD5 authentication encryption sequence that is lower than previous sequence number.
470657	Kernel NULL pointer de-referenced on both the devices of FG-3700D cluster.
473468	All members of a two-unit cluster takes on a slave role after adding port with status `down` and rebooting the master.
474088	Kernel panic and reboot after upgrading FG-400D cluster to 5.6.3.

IPS

Bug ID	Description
460417	High CPU caused by `ipsengine 03.430 *** signal 14 (Alarm clock) received ***`.
463402	Application control of FG-200E works abnormally.
469608	ICMP packets dropped during FortiGate update.
477735	`ipsengine` crash at signal 11.

IPsec VPN

Bug ID	Description
459640	OSPF over IPsec tunnel not getting established after VPN restart.
462203	IPsec performance decreased with FG-100D after upgrade to 5.6.2.
465323	After reconnecting IPsec tunnel, IPsec local and remote interface addresses are not installed on SPOKE's routing table.
466314	The IPsec phase1 `psksecret` setting is lost after upgrading from 5.4.x to 5.6.0 or 5.6.3. Upgrading to 5.6.1, 5.6.2, or 5.6.4 has no issue.
475751	Encrypted traffic doesn't go through the IPsec tunnel.
476198	IPsec traffic sourced from FW interface not processed correctly by policy.
476461	IKE does not release the `mode-cfg framed-IP` assigned from RADIUS.
482622	Traffic Selector issues with IKEv2 in transport-mode and NAT.

Log & Report

Bug ID	Description
416790	"(no.x pattern matched)" is not logged when BWL matches envelop MAIL FROM.
443619	Missing `direction=` in the application control logs.

Proxy

Bug ID	Description
460183	Some sites may be re-signed by an untrusted CA when SSL inspection is enabled on FortiGate.
463420	WAD crashes when user is stale.
463427	WAD crashes when HTTPS post is blocked.

Bug ID	Description
463908	WAD enters conserve mode by its own memory calculation.
464023	WAD crashes when HTTPS with no SNI hits an IPv4 policy with `http-policy-redirect` and then finalizes with a transparent web.
466146	Server certificate is always untrusted if the IPC fails between WAD and `fnbamd`.
466294	Suggests using `fnbamd` to implement the resending mechanism when there's `sendto` error.
466879	SSL handshake fails sporadically when security profile in proxy mode is applied.
469217	IPS and proxy can't verify certificate signed by *VeriSign Class 3 Public Primary Certification Authority - G3*.
469656	WAD crashes when `inspect-all` is enabled.
470580	WAD memory leak for LDAP authentication.
471189	All scanunit daemons are killed after proxy-policy configuration is changed.
473976	WAD process keeps crashing when AV proxy inspection (with third-party explicit proxy traffic) is enabled.

Router

Bug ID	Description
454871	OSPFD crash signal 11 `ospf_external_lsa_refresh`.
457886	SDWAN rules will match traffic not destined for SDWAN interfaces.
460624	OSVFv3 doesn't inject external route tag field into LSU (LSA 5).
460808	VRRP packets coming from wan1 are not be forwarded to wan2.
462457	Kernel routes learnt from old ELBC master never expire on worker blade that are never master.
468451	Multicast flow takes 10 seconds to be forwarded if the receiver joins the group first.
476370	OSPFv3 doesn't consider forward metric for E2 routes to ASBR with interface cost statement.

Spam

Bug ID	Description
466606	Emails tagged as SPAM - Whitelist is not effective.

SSL VPN

Bug ID	Description
130461	FortiGate queries RADIUS server too many times when *include in all groups* is enabled in RADIUS server configuration.
399784	URL modified incorrectly for a dropdown list in application server.
424561	SSL VPN web mode has trouble loading certain page in HTTP/HTTPS bookmark.
440853	RDP over web-mode SSL VPN to a Windows server changes the time zone to GMT.
441068	SSL VPN unable to connect in tunnel mode, seeing multiple stale sessions for the same user.
441517	RDP and VNC using interface IP address for NAT instead of IP Pool when opened from SSL portal.
458686	RDP fails in SSL VPN if policy with FQDN object is on top.
460145	SSL VPN user is not prompted for a token.
460401	Images on Internet websites do not load properly when accessed through SSL VPN web mode.
469132	Unable to view the nagivation tab when accessing `http://test-wiki.intence.local/xwiki` via SSL VPN web based mode.

System

Bug ID	Description
444969	Memory utilization is high on FG-300D.
450389	IPv6 problem with neighbor-cache.
452456	Memory leak on FG-100D slave unit.
457004	DHCP Relay sends too many DHCP Offers to client.
460385	Kernel panic on FG-201E v5.4.6.
461989	ESP traffic is not forwarded out via inter-VDOM link.
464332	SNMP agent returns `No Such Object available` when querying `etherStatsCRCAlignErrors` MIB variable.
466435	Cross NP traffic on a VLAN interface configured over Aggregate interface is not forwarded.
469658	VLAN interface configured under VDOM is lost while restoring the VDOM config.
469821	In TP mode, a few packets are not captured through `diag sniffer packet`.
470160	CLI commands via SSH does not give correct output when admin user has 2 FA enabled (FortiToken).
470408	Cannot create new VDOM even though a license extension has been added to both cluster units.

Bug ID	Description
471626	`dot3StatsFCSErrors` MIB OID query systematically returns `0` despite CRC errors recorded in `rx_crc_error` counter.
472716	Cannot delete entry in `system.mac-address-table`.
472903	FG-3960E single mode QSFP28 100G link does not come up after chassis reboot.
475539	Inaccurate netflow export, traffic measurements do not match with SNMP readings.

Switch

Bug ID	Description
467235	`fnbamd` crashes after enabling the `security-mac-auth-bypass` feature in wired interface.

Table Size

Bug ID	Description
486907	Increase table size of `router.rip:offset-list`.

Upgrade

Bug ID	Description
478622	`vdom_links` of virtual cluster2 VDOMs getting deleted after firmware upgrade from 5.4.5 to 5.6.3.

VM

Bug ID	Description
462209	Checksum mismatch on master and backup FGT-VM64 (VM00) over ESXi 6.0.

WebProxy

Bug ID	Description
459504	File upload does not work on FTP over HTTP when security profile is configured.
464101	WAD crashes at signal 11,
469640	Firewall policy authentication redirection URL is incorrect for webproxy traffic.
473515	WAD process crashes with signal 11.
474259	SOCKS proxy does not respect assigned `outgoing-ip` in proxy setting (secondary IP address of the external interface).

Bug ID	Description
476708	Internal WAD user counter gets stuck.

WiFi

Bug ID	Description
462875	`hostapd` crashes with `*** signal 11 (Segmentation fault) received ***`.
467501	`cw_acd` crashes on FG-900D causes all FortiLink FSWs to go off-line.
467758	Not able to pass data traffic when DTLS policy is set to clear text.

Common Vulnerabilities and Exposures

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

Bug ID	Description
440744	FortiOS 5.6.4 is no longer vulnerable to the following CVE Reference: • CVE-2017-7739
454452	FortiOS 5.6.4 is no longer vulnerable to the following CVE Reference: • CVE-2016-2183
458880	FortiOS 5.6.4 is no longer vulnerable to the following CVE Reference: • CVE-2017-14190

Known Issues

The following issues have been identified in version 5.6.4. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
435951	Traffic keeps going through the `DENY` NGFW policy configured with URL category.
448247	Traffic-shaper in shaping policy does not work for specific application category like as P2P.

AV

Bug ID	Description
446204	The filename of character in Korean shows mismatch encoding type in GUI.

FIPS-CC

Bug ID	Description
463211	When alarm is enabled in FIPS mode, the console hangs and the `getty` process uses very high CPU usage.

FortiGate-90E/91E

Bug ID	Description
393139	Software switch span doesn't work on this platform.
424212	FG-90E can't receive packets from span ports.

FortiGate 500D

Bug ID	Description
403449	FortiGate 500D has some issue with FINISAR transceiver.

FortiGate 3815D

Bug ID	Description
385860	FG-3815D does not support 1GE SFP transceivers.

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	HA with FortiLink traffic loss – no virtual MAC.
357360	DHCP snooping may not work on IPv6.
369099	FortiSwitch authorizes successfully, but fails to pass traffic until you reboot FortiSwitch.
404399	FortiLink goes down when connecting to ForiSwitch 3.4.2 b192.
408082	Operating a dedicated hardware switch into FortiLink changes STP from *enable* to *disable* in a hidden way.
462080	FG-300E reboots with kernel panic errors.
477885	FSW Security Policy – RADIUS configuration not pushed to FSW if `source-ip` is specified. Workaround: configure a separate RADIUS server without `source-ip` parameter and use it in the FSW security policy.

FortiView

Bug ID	Description
366627	FortiView Cloud Application may display incorrect drill down *File and Session* list in the *Applications View*.
368644	*Physical Topology: Physical Connection* of stacked FortiSwitch may be incorrect.
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
408100	Log fields are not aligned with columns after drill down on FortiView and Log details.
441835	Drill down a `auth-failed` wifi client entry in "Failed Authentication" could not display detail logs when CSF enabled.
442238	FortiView VPN map can’t display Google map (199 dialup VPN tunnel).
442367	In *FortiView* > *Cloud Applications*, when the cloud users column is empty, drill down will not load.

GUI

Bug ID	Description
356174	FortiGuard `updategrp` read-write privilege admin cannot open FortiGuard page.
374844	Should show `ipv6` address when set `ipv6` mode to `pppoe/dhcp` on *GUI* > *Network* > *Interfaces*.
375383	If the policy includes the *wan-load-balance* interface, the policy list page may receive a javascript error when clicking the search box.

Bug ID	Description
422413	Use API monitor to get data for FortiToken list page.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
445113	IPS engine 3.428 on Fortigate sometimes cannot detect Psiphon packets that iscan can detect.
451776	Admin GUI has limit of 10 characters for OTP.

HA

Bug ID	Description
458320	Cluster uptime was not consistent.
479311	Certificate status changes from *OK* to *Pending* one minute after importing certificate from GUI on vcluster device.

IPS

Bug ID	Description
443418	User is not listed in quarantine list in case `block duration` value is set long enough.
450693	`ERR_SSL_PROTOCOL_ERROR` when deep scan enabled along with IPS in policy.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create webfilter logs.
438858	Synchronized log destination with *Log View* and *FortiView* display source.

Proxy

Bug ID	Description
454185	Specific application does not work when deep inspection is enabled.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
411368	In FortiView with FortiAnalyzer, the combined MAC address is displayed in the *Device* field.

Bug ID	Description
414013	Log Settings shows `Internal CLI error` when enabling historical FortiView at the same time as disk logging.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.

System

Bug ID	Description
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
435388	The parent physical interface cannot be in zone list when VLAN interface is added to zone.
436580	`PDQ_ISW_SSE` drops at +/-100K CPS on FG-3700D with FOS 5.4 only.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
440411	Monitor NP6 IPsec engine status.
457096	FortiGate to FortiManager tunnel (FGFM) using the wrong source IP when multiple paths exist.
459273	Slave worker blade loses local administrator accounts.
486466	HTTPS web page is blocked after clicking *Proceed* button.

VM

Bug ID	Description
441129	Certify FortiGate-VMX v5.6 with NSX v6.3 and vSphere v6.5.
476617	AWS and AWSONDEAMAND instance deployed with NVMe type disks cannot upgrade. Workaround: On existing 5.6.4 instance with AWS C5 type, issue this command before upgrade: `fnsysctl ln -s /dev/nvme0n1p1 /dev/nvme0n11`

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.

Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.