FortiOS - Release Notes

Version 6.0.5

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/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: techdoc@fortinet.com

May 30, 2019
FortiOS 6.0.5 Release Notes
01-605-553329-20190530

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-05-14	Initial release.
2019-05-15	Added 490447 to Resolved Issues.
2019-05-24	Moved 532015 from Known Issues to Resolved Issues.
2019-05-27	Updated 539553 in Resolved Issues.
2019-05-30	Deleted 451776, 479987, and 528767 from Known Issues.

Introduction

This document provides the following information for FortiOS 6.0.5 build 0268:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.0.5 supports the following models.

FortiGate	FG-30D, FG-30D-POE, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, 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-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-30D, FWF-30D-POE, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VMX, FG-VM64-XEN, FG-VM64-GCP, FG-VM64-OPC, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCPONDEMAND
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 6.0.5 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 6.0.5. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0268.

FG-400E	is released on build 6164.
FG-401E	is released on build 6164.
FG-600E	is released on build 6164.
FG-601E	is released on build 6164.
FG-3400E	is released on build 6174.
FG-3401E	is released on build 6174.
FG-3600E	is released on build 6174.
FG-3601E	is released on build 6174.
FG-VM64-RAXONDEMAND	is released on build 8242.

Special Notices

WAN optimization and web caching functions

WAN optimization and web caching functions are removed from 60D and 90D series platforms, starting from 6.0.0 due to their limited disk size. Platforms affected are:

- FGT-60D
- FGT-60D-POE
- FWF-60D
- FWF-60D-POE
- FGT-90D
- FGT-90D-POE
- FWF-90D
- FWF-90D-POE
- FGT-94D-POE

Upon upgrading from 5.6 patches to 6.0.0, `diagnose debug config-error-log read` will show command parse error about `wanopt` and `webcache` settings.

FortiGuard Security Rating Service

Not all FortiGate models can support running the FortiGuard Security Rating Service as a Fabric "root" device. The following FortiGate platforms can run the FortiGuard Security Rating Service when added to an existing Fortinet Security Fabric managed by a supported FortiGate model:

- FGR-30D-A
- FGR-30D
- FGR-35D
- FGR-60D
- FGR-90D
- FGT-200D

- FGT-200D-POE
- FGT-240D
- FGT-240D-POE
- FGT-280D-POE
- FGT-30D
- FGT-30D-POE
- FGT-30E
- FGT-30E-MI
- FGT-30E-MN
- FGT-50E
- FGT-51E
- FGT-52E
- FGT-60D
- FGT-60D-POE
- FGT-70D
- FGT-70D-POE
- FGT-90D
- FGT-90D-POE
- FGT-94D-POE
- FGT-98D-POE
- FWF-30D
- FWF-30D-POE
- FWF-30E
- FWF-30E-MI
- FWF-30E-MN
- FWF-50E-2R
- FWF-50E
- FWF-51E
- FWF-60D
- FWF-60D-POE
- FWF-90D
- FWF-90D-POE
- FWF-92D

Built-in certificate

FortiGate and FortiWiFi D-series and above have 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.

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

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.

Using FortiAnalyzer units running older versions

When using FortiOS 6.0.5 with FortiAnalyzer units running 5.6.5 or lower, or 6.0.0-6.0.2, FortiAnalyzer might report increased bandwidth and session counts if there are sessions that last longer than two minutes.

For accurate bandwidth and session counts, upgrade the FortiAnalyzer unit to 6.0.5.

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

- FortiAnalyzer 6.0.0 and later
- FortiClient 6.0.0 and later
- FortiClient EMS 6.0.0 and later
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.4 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*.

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.0.5. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.5 and some running 5.6.x.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.0.5 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.0.5 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

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 6.0.5 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 6.0.5 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*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

Product Integration and Support

The following table lists FortiOS 6.0.5 product integration and support information:

Web Browsers	• Microsoft Edge 44 • Mozilla Firefox version 66 • Google Chrome version 73 • Apple Safari version 12.1 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 41 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 59 • Google Chrome version 65 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in . 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 . For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.0.0 See important compatibility information in Fortinet Security Fabric upgrade on page 11. If you're upgrading both FortiOS and FortiClient from 5.6 to 6.0, upgrade FortiClient first to avoid compatibility issues. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 5.6.0 and later
FortiClient Android and FortiClient VPN Android	• 5.4.2 and later
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 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 0276 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

FortiExtender	• 3.3.2, 4.0.0
AV Engine	• 6.00019
IPS Engine	• 4.00035
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, 2012 R2, and 2016
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, 6.5, and 6.7
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 (32-bit & 64-bit)	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)	Mozilla Firefox version 66 Google Chrome version 73
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 66 Google Chrome version 73
Linux Ubuntu 16.04 / 18.04 (32-bit & 64-bit)	Mozilla Firefox version 66
MacOS High Sierra 10.13.6	Apple Safari version 12 Mozilla Firefox version 66 Google Chrome version 72
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

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✔	✔
Kaspersky Antivirus 2009	✔	
McAfee Security Center 8.1	✔	✔
Trend Micro Internet Security Pro	✔	✔
F-Secure Internet Security 2009	✔	✔

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✔	✔
AVG Internet Security 2011		
F-Secure Internet Security 2011	✔	✔
Kaspersky Internet Security 2011	✔	✔
McAfee Internet Security 2011	✔	✔
Norton 360™ Version 4.0	✔	✔
Norton™ Internet Security 2011	✔	✔
Panda Internet Security 2011	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Resolved Issues

The following issues have been fixed in version 6.0.5. For inquires about a particular bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
519759	Process `scanunit` crashes in `removeTransformCleanup` when Outbreak prevention is enabled.
525711	FortiGate not sending email headers to FortiSandbox.
530210	Content Disarm cleans file even when it what was flagged Clean in FortiSandbox.

Data Leak Prevention

Bug ID	Description
518146	DLP incorrectly blocking .deb file extension (DLP log unclear for matches in archive files).
524910	DLP profile to block the file name pattern "*" not blocking uploaded files.
530470	DLP blocking `html` file categorized as `bat` file.

DNS Filter

Bug ID	Description
525068	No need to resolve safe search FQDN if not used.

Endpoint Control

Bug ID	Description
521645	Traffic blocked after enabling *Compliance* on SSL VPN interface.
525179	FortiGate fails to assign FortiClient Compliance profile based on LDAP group membership.

Firewall

Bug ID	Description
492034	Traffic not matching expected sessions and getting denied.
525995	Session marked dirty when routing table update for route which is not related to the session.

Bug ID	Description
526748	Firewall policies with action DENY show `Default` proxy-options applied in GUI.
528464	Disappearing policy add. Also happens in 6.0.3 build 0200.
536868	A FortiGate in TP mode with set `send-deny-packet` enabled policy, generates strange ICMP-REPLY for TCP SYN/ICMP-REQUEST/UD.

FOC

Bug ID	Description
536520	GTP Tunnel States are not synced on subordinate unit after a reboot.

FortiView

Bug ID	Description
521497	The FortiView All Sessions real time view is missing right-click menu to end `session/ban ip`.
527708	Policy ID hyper link in policy view is missing.
527751	No user name on *Fortiview* > *Sources* main page
527775	FortiView logs entries do not refresh on log drill down page.
527952	*FortiView* > *WiFi Clients* > *drill down* > *Sessions* gets nothing at final drill down if device identification is disabled.
528684	*FortiView* > *Bubble Chart* cannot drill down on Firefox 63 with ReferenceError: "event is not defined".
528744	*FortiView* > *Traffic Shaping* displays data with error message if switched from other pages in custom period.
529313	*FortiView* > *Web Sites* > *Web Categories* drill down displays all entries in *Policies* tab.
529558	*System Events* widget shows *No matching entries found* when drilling down HA event.
538873	Traffic shaper info missing under Shaper column in FortiView.
539981	Unable to see Source DNS Name in FortiView.

GUI

Bug ID	Description
473148	FGT5001D Sessions widget in Dashboard show negative % for nTurbo after throughput test.
477493	GUI fails to read correct Last Used time for firewall policy.
479482	Timeout does not work properly if user moves away from FortiGate GUI.
493704	While accessing FortiGate page, browser memory usage keeps spiking and finally PC hangs.

Bug ID	Description
498738	GUI creating B/W widget referencing SIT-Tunnel generates error.
509791	Editing Address Objects name within SSL-SSH inspection profile selection pane cause loss of Address/Web exemption objects.
509978	Unable to download the results of the scheduled script.
521253	LAG interface is not listed on the dropdown list when configuring DNS Service.
536841	DNS server in VPN SSL setting is overwritten when SSL-VPN settings are modified via GUI.

HA

Bug ID	Description
494900	Interface faceplate on *System* > *HA* shows inconsistent port link status with interface faceplate on *Network* > *Interface*.
513940	Enormous amount of session between heartbeat Interfaces for port 703 (HASYNC).
516234	GUI checksums show slave is not synchronized when the master is synchronized.
518717	MTU of session-sync-dev does not come into effect.
526252	High memory caused by updated daemon.
526492	FGSP between two FGCP clusters - session expectation.
526703	FGSP of FGCP cluster, does not pickup NAT'ed sessions.
529274	Factory reset box faild to sync with master in multi-VDOM upgraded from 6.0.3.
530215	Application `hasync *** signal 11 (Segmentation fault) received ***`.
532015	High CPU on Core1 due to session sync process.
538289	Old master keeps forwarding traffic after failover.
541224	Network loop over virtual-wire-pair in HA mode if running diagnose `sys ha reset-uptime`.
547700	HA out of sync after upgraded in multi-VDOM environment.

Intrusion Prevention

Bug ID	Description
452131	`ipsengine` up time on FG-51E is a negative number after changing db from extended to regular.
476219	Delay for BFD in IPinIP traffic hitting policy with IPS while IPsec calculates new key.
525398	Disabled and enabled IPS Signatures looks the same in IPS Sensor GUI.
528860	IPS archive PCAP periodically cannot capture.

IPsec VPN

Bug ID	Description
514519	OSPF neighbor can't up because IPsec tunnel interface MTU keeps changing.
518063	DPD shows unnegotiated and is not functioning correctly on ADVPN Spoke.
519187	IKE route should not be deleted if it is needed by other `proxyids`.
527137	Local GW disappears from GUI.
537140	KEv2 EAP - FortiGate fails to respond to IKE_AUTH when ECDSA certificate is used by ForitGate.
537450	Site-to-site VPN policy based - with DDNS destination fail to connect.
537769	FortiGate sends failure response to L2TP CHAP authentication attempt before checking it against RADIUS server.

Log & Report

Bug ID	Description
387324	Archive mark is always on under UTM logs page when log-display location set to FAZ.
521020	VPN usage duration days in local report is not correct.
528786	In Log viewer, forward traffic filter Result Accept(all)/Deny(all) does not work.

Proxy

Bug ID	Description
458057	Constant DNS query on built-in FQDN cause network congestion.
470407	IPv6-Happy-Eyeballs-Mechanism not working with proxy-based Webfilter-Profile.
491675	FTP Server is not accessible when AV profile is set to proxy based inspection.
512936	SSL certificate inspection in proxy mode doesn't use CN from Valid Certificate for categorization when SNI is not present.
516863	Webproxy learn-client-ip webfilter's auth/warn/ovrd does not work.
525518	Skype call drops when handled by WAD process after around three sec of being answered.
526667	FortiGate doesn't forward `request:port` command after 0 byte file transmission.
531575	Web site access failure due to OCSP check in WAD + Deep SSL inspection.
532121	WAD uses high CPU with "netlink recvmsg No buffer space available" after upgrade to 6.0.3+.
533838	WAD re-signs valid web sites with Untrusted CA certificate.
534346	WAD memory leak on OCSP certificate caching.
539452	FortiGate does not follow Authority key identifier when sending certificate chain in deep inspection.

Bug ID	Description
544517	WAD process crashing and affecting HTTP/HTTPS traffic.
545964	FortiManager sends requests to FortiGate to collect proxy policy hit_count/bytes, and the response from FortiGate misses the `uuid` attribute.
549787	Unable to fetch the Root and Intermediate Certificate.

REST API

Bug ID	Description
523902	REST API issue: Access Token only verifies the first 30 characters.

Routing

Bug ID	Description
526008	Differences between routing table and kernel forward information. ADVPN + BGP.
527478	Proute list fill "null " application name.
528465	GRE tunnel does not come up.
529683	Upgrade from 5.6 to 6.0 causes all routes to be advertised in BGP.
531660	With VRRP use VRDST checking without default gateway.
531947	SD WAN IPsec interfaces keep failing over when link selection strategy is set to Custom-profile.
533018	Process `nsm` with high CPU when displaying the GUI section of IP4 and IPv6 policy when receiving full routing of BGP.
537110	BGP/BFD packets marked as CS0.
539982	Multicast failed after failover from another interface.
541072	BGPd crash.
544603	Multicast on interfaces with secondary IP addresses.
546198	SD-WAN performance SLA via GRE-Tunnel fails to set options or connect ping6 socket for monitor.

Security Fabric

Bug ID	Description
525790	Not able to connect through SSL VPN to addresses resolved by SDN dynamic objects.

SSL VPN

Bug ID	Description
493127	Connection to web server freezes when using SSL VPN web bookmark.
509333	SSL VPN to Nextcloud doesn't open.
515370	SSL VPN access denied if address object added after group object in firewall policy.
517819	Unable to load web page in SSL VPN web mode.
517859	Unable to load web page for some internal web sites in SSL VPN web mode.
518406	Unable to load WebPage through SSL VPN webmode. Some js files of xunta internal web sites have problems.
519113	SSL VPN web mode SMB connection doesn't work when enable then disable SMBCD debug.
520965	IBM QRadar page not displaying in SSL VPN web-mode.
521036	SSL VPN web mode access problem.
522987	Backup and restore the VDOM config with SSL VPN settings causes some critical flags and counter for SSL VPN to not update so SSL VPN stops working.
523450	Unable to access internal website via bookmark in SSL VPN web mode.
523647	Search result gives empty output upon accessing the URL *https://ieeexplore.ieee.org* via SSL VPN bookmark.
523717	Dropdown list can not get expanded through bookmarks (SSL VPN).
525375	Atlassian Confluence wiki Javascript problem via SSL VPN web mode.
527348	JavaScript script is not available when connecting using SSL VPN web mode.
527476	Update from web mode fails for SharePoint page using MS NLB.
528289	SSL VPN crashes when it receives HTTP request with header "X-Forwarded-For" because of the wrong use of `sslvpn_ap_pstrcat`.
529186	Problem loading reaching internal web server through SSL VPN Web bookmark when using HTTPS. Some js files of "srvdnsmgt" do not run correctly.
529512	SSL VPN user gets disconnected when load-balance-mode is measured-volume-based in SD-WAN.
530223	SSL VPN wants client certificate even when no client-cert for realm is configured.
530833	Synology NAS login page stuck after login when accessing by SSL VPN Web portal.
531827	Active cache memory leak after upgrade to 6.0.3 GA.
531848	FortiSIEM WebGUI does not load on web portal.
533008	SSL web mode is not modifying links on certain web pages.
536058	Redirected port is not entered in the URL through SSL VPN web mode.
538904	Unable to receive SSL tunnel IP address.

Bug ID	Description
539187	SSL VPN random stale sessions exhausting IP pool.
546161	TX packet drops on ssl.root interface.

Switch Controller

Bug ID	Description
490447	Multiple fortilinks flapped during staging upgrade.
527521	On FortiSwitch Ports page, Display More does not work.
530237	HA cluster out-of-sync after changing port POE mode on switch-controller managed-switch settings: Double commit.

System

Bug ID	Description
370151	CPU doesn't remove dirty flag when returns session back to NP6.
466805	Adding USB Host devices to a virtual machine connected by USB to FortiGate 500D causes the units to restart in loop.
468684	EHP drop improvement for units using NP_SERVICE_MODULE.
479533	`skippingBad tar header` message flooding on console after rebooting box and retrieving logs.
492655	DNSproxy does not seem to update link-monitor module.
493128	`bcm.user` always takes nearly 70% CPU after running Nturbo over IPsec script.
496934	New feature merge: DNS Domain List.
505252	EMAC VLAN: SNMP data is incorrect.
505522	Intermittent failure of DHCP address assignment.
510973	FortiGate with disk and send logs to FAZ has PCI alerts.
511018	SSH/SSL VPN connection to external VLAN interface drop by changing unrelated interface IP or restart OSPF.
513419	High CPU on some cores of CPU & packet drops around 2-3%.
519246	`ipmc_sensord` process not checking sensors due to pending jobs.
519493	MCLAG: if remote side change systemID, only one port goes down, the other remains up.
521193	DNSPROXY causing high CPU usage.
524422	Merge br_6-0_sp back to 6.0 and 6.2.
525813	FortiGate managed by FortiManager intermittently going offline after rebooting FortiGate.
526646	LAG interface flaps when the member ports go up.

Bug ID	Description
526771	Allow sit-tunnel to not specify the source address.
526788	Password policy forces password change even if expire-status is disabled.
527390	Kernel panic in the HA cluster with FortiGate-3800D units running FortiOS v6.0.0 build 0200
527902	TXT records are truncated in DNS replies, when FortiGate is used as DNS server.
528004	Add global log device statistics to SNMP.
529932	Primary DNS server is not queried even after 30 seconds.
531584	Kernel Panic when Fragmented Multicast Traffic received on EMAC-VLAN interface.
533556	Read-only admin account can delete IPsec SA.
534757	Device 80D reboots every 2-3 days with a kernel panic error.
535730	Memory leak after upgrade to 6.0.4.
536817	FortiGate sending DHCP offer using broadcast.
538304	Aggregate interface (four member) flapps when the third member interface goes down.
539090	Modifying FortiGate administrator password to complex ones via SSH triggers a FortiManager password change by auto-update.
539444	5001D blade rebooted on its own due to kernel panic.
542441	SNMP monitoring of the implicit deny policy not possible.
547720	FortiGate does not support DH 1024 bits as SSH server.

Upgrade

Bug ID	Description
498396	Upgrade from 5.2.13 to 5.4.9 is affected by application list global limit.
530793	`config-error-log` shows after upgrade from v5.6.6 to v5.6.7.
546874	Increase firewall.address tablesize for 80-90 series.

User & Device

Bug ID	Description
517702	VPN certificate CA: shows newly added entry before reboot but not after.
525648	FortiOS does not prompt for token when Access-Challenge is received - RADIUS authentication fails.
525925	Unable to login to FortiGate using Symantec 2-factor authentication.
525929	LDAPS requests fail with fnbamd stop error "Not enough bytes". LDAP works fine. Additional timeout observed.

Bug ID	Description
529945	Local certificate content changes should be directly applied for the admin-server-cert sent to the client browser.
535279	FortiGate sends error user password to RADIUS server for CMCC auth user sometimes.

VM

Bug ID	Description
526471	VMX: Adding a security group with ~30+ devices into the redirection policy the connection starts to experience huge delay.
540062	Kernel panic after upgrade from 5.6.7 to 5.6.8.
542794	`Session size overflow` on VMX causing timeout and error on NSX vMotion task.

WCCP

Bug ID	Description
529685	WCCP not use the tunnel.

Web Filter

Bug ID	Description
509860	Regex case insensitivity flag is ignored in 5.6.5 and 6.0.2 when FortiGate is in proxy mode.
518433	FGT D series number of web filter profiles decreased globally.
531101	Web Filter inspection proxy mode unable to resolve hostname because website is unrated.
541539	URL filter wildcard expression not matched correctly on proxy mode.
544598	Invalid hostname return on GUI when static URL is defined.

WiFi Controller

Bug ID	Description
516067	CAPWAP traffic from non-VLAN SSID is blocked when `dtls-policy=ipsec-vpn` and NP6 offload are enabled.
530328	CAPWAP traffic dropped when offloaded if packets are fragmented.
537848	FortiGate IPsec VPN phase1-interface and phase2-interface configurations are not saved into configuration file.
537968	Region -N DFS support required for FAP-U422EV.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
452730	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2017-14186
496642	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2018-13371
528040	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2018-13384
529353	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2018-13380
529377	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2018-13379
529712	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2018-13381
529719	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2018-13383
529745	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2018-13382
534592	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2019-5587
539553	FortiOS 6.0.5 is no longer vulnerable to the following CVE Reference: • CVE-2019-5586 • CVE-2019-5588

Known Issues

The following issues have been identified in version 6.0.5. 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.
488369	DSCP/ToS is not implemented in shaping-policy yet.

Firewall

Bug ID	Description
546145	If the firewall policy includes a nonexistent ISDB ID on updated ISDB version, the firewall policy is not read and reflected.
554806	Deleted policy entry on interface pair view doesn't disappear until refresh page.

FortiView

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.
525702	FortiView does not support auto update in real-time view and shows unscanned application.
526956	FortiView widgets get deleted on upgrading to B222.
527540	In many FortiView pages, the *Quarantine Host* option is not clickable on a registered device.
528483	*FortiView* > *Destination* page filter *destination owner* cannot filter out correct destination in real time view.
554791	Policy direct hyperlink from historical FortiView sessions does not highlight policy.

GUI

Bug ID	Description
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
508015	Edit Policy from GUI changes `fsso` setting to disabled.

Bug ID	Description
516415	*Edit Disclaimer Message* button is missing on *Proxy Policy* page.
548775	Cannot continue to configure the same column for different ports in FortiSwitch Ports page unless you refresh the page.

HA

Bug ID	Description
539155	HA master does not send SNMP trap when plugging cable into interface that is set as `ha-mgmt-interfaces`.

Intrusion Prevention

Bug ID	Description
445113	IPS engine 3.428 on FortiGate sometimes cannot detect Psiphon packets that iscan can detect.

IPsec VPN

Bug ID	Description
469798	The interface shaping with egress shaping profile doesn't work for offloaded traffic.
481201	The OCVPN feature is delayed about one day after registering on FortiCare.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create web filter logs.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.
554821	SSL VPN web mode to FortiGate 6.2 and 6.0.4 has display problem.

Switch Controller

Bug ID	Description
357360	DHCP snooping may not work on IPv6.

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.
472843	When FortiManager is set for `DM = set verify-install-disable`, FortiGate does not always save script changes.
474132	FG-51E hang under stress test since build 0050.

Upgrade

Bug ID	Description
470575	After upgrading from 5.6.3, `g-sniffer-profile` and `sniffer-profile` exist for IPS and web filter.
473075	When upgrading, multicast policies are lost when there is a zone member as interface.
481408	When upgrading from 5.6.3 to 6.0.0, the IPv6 policy is lost if there is SD-WAN member as interface.
494217	Peer user SSL VPN personal bookmarks do not show when upgrade to 6.0.1. **Workaround**: Use CLI to rename the user bookmark to the new name.

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.