FortiOS - Release Notes

Version 6.0.2

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

July 26, 2018
FortiOS 6.0.2 Release Notes
01-602-502422-20180726

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-07-26	Initial release.

Introduction

This document provides the following information for FortiOS 6.0.2 build 0163:

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

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.0.2 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-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-5001D, FG-3960E, FG-3980E, 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-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, 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 6.0.2 images are delivered upon request and are not available on the customer support firmware download page.

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 mode:

- 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.

Upgrade Information

Upgrading to FortiOS 6.0.2

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 or 5.6.3, 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.

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.

Fortinet Security Fabric upgrade

FortiOS 6.0.2 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.0.0
- FortiClient 6.0.0
- FortiClient EMS 6.0.0
- 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 6.0.2. When Security Fabric is enabled, you cannot have some FortiGate devices running 6.0.2 and some running 5.6.x.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.0.2 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 6.0.2 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 6.0.2 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 6.0.2 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

FortiOS 6.0.2 support

The following table lists 6.0.2 product integration and support information:

Web Browsers	• Microsoft Edge 41 • 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.
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 Fortinet 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 Fortinet 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** • **Mac OS X** • **Linux**	• 6.0.0 See important compatibility information in Fortinet Security Fabric upgrade on page 10. If FortiClient is being managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate. 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)	• 3.6.4 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 0268 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	• 3.2.1
AV Engine	• 6.00012
IPS Engine	• 4.00021
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
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
OS X El Capitan 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

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 6.0.2. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
487946	MSS value increases when AV or WEB filter in use resulting in `Packet too big` message.
489308	`scanunit` process frequently crashes.
497371	Flow-AV blocks Windows updates (.cab files).

Application Control

Bug ID	Description
423140	All IPS sessions lost when new custom signature added.

Authentication & User

Bug ID	Description
477392	Cannot use FAC username password and FortiToken two-factor authenticate login HA slave unit.
481469	Failed to resolve hostname for configured CRL URL on a non-managment VDOM.
488566	Renaming guest user group name doesn't reflect under Guest administrator account assigned leads to black page.
491175	`diag test application fnbamd 1` causes `fnbamd` to enter an idle state and causes authentication failure.
491235	New `diag` command `diag test app wad 13`.
491241	Enhance `diag` command `diag test app fnbamd 1`.
493470	Authenticated user receives *Oops "Authentication requested"* referencing a proxy policy which does not have authentication.
493930	Admins who use dedicated HA mgmt interfaces are not visible in the CLI.
495210	Guest user accounts do not show expiration time, but time until expiration only.
496524	After successful wired portal auth, the wired PC still gets many http redirection and fails to access the internet.

Connectivity

Bug ID	Description
463982	FortiManager IP is unset in FortiGate CM.
479607	Scheduled auto-update happens twice in 10 seconds but a log entry for the first try is not logged.
481058	Configuration revision control list can't be retrieved from FortiCloud.

DLP

Bug ID	Description
478524	Diskless model missing `full-archive-proto` in config DLP sensor when only FortiCloud logging enabled.
486958	Scanunit signal 14 alarm clock caused by DLP scanning bz2 file.
492624	DLP blocking web sites in FortiOS v6.0 GA.
496255	Some XML-based MS Office files are recognized as ZIP files.

Firewall

Bug ID	Description
474612	SNAT is using low ports below 1023.
475539	Inaccurate netflow export. Traffic measurements do not match with SNMP readings.
478681	Should be able to disable SNAT when a VIP exists and central-NAT is enabled.
492961	Set `utm-status disable` did not hide profile-group. Unset `profile-group` will make `profile-protocol-options` empty.
498188	`Dirty_session_check` in FortiGate drops all established VIP64 sessions.
502579	Local-In-Policies with FQDN address is not working after upgrade from 5.6 to 6.0.1.

FortiView

Bug ID	Description
414172	HTTPsd / DNSproxy/ high CPU/memory with high rate UDP 1Byte spoofing traffic.

GUI

Bug ID	Description
402457	Suggest to improve IPsec VPN monitor page *Proxy ID Source* and *Proxy ID Destination* fields.

Bug ID	Description
413881	VDOM link tooltip displays *Failed to retrieve info*.
444104	Accept/Decline buttons cannot be seen in GUI with a long login disclaimer and screen under certain resolutions.
449598	*Remote LDAP User Definition* wizard does not pull users.
457627	Want the ability to change the date/time format displayed in the GUI of the FortiGate.
457721	FortiLink Switch-controller GUI - allow user to edit Port Description for FortiLink/ISL.
457966	Virtual wire pair > Add VLAN range filter on GUI.
460617	GUI FortiGuard *Check Again* button doesn't work as expected due to FortiGuard service 8888/53 incorrectly routed.
462011	GUI is blank when accessed with RADIUS user with read-access profile and the FortiGate is managed by FortiManager.
462072	GUI should show full FQDN name in reputation search result.
468465	Some filters do not return logs when source is FortiCloud.
468797	Cannot filter by date or timestamp when viewing logs from FortiCloud.
469082	*prof_admin* profile admins are not able to display GUI IPv4 source address.
470241	Raw logs are downloaded from the default location even if you select another log device in GUI.
472023	Outbreak prevention detection makes "clean" counter increment in *Advanced Threat Protection Stats* widget.
472558	DHCP Server GUI - GUI populates wrong information when switching from DHCP Relay to DHCP Server.
473808	Column filter is not persistent and is removed after refreshing the page.
474807	Cannot restore default page in replacement message group.
475036	*Virtual Server Duplicate Entry found* error in GUI.
477393	Negative values in *Load Balance* monitor logs.
477870	Alias for modem interface present in GUI but not in CLI.
479468	The link status is lost after SD-WAN GUI changes to *List Edit*.
479937	GUI should hide options that don't apply to certificate inspection.
481902	When accessing *FortiView* > *Websites* page, gets error *Failed to get FortiView data* and httpsd keeps crashing.
482628	`CPU.Speculative.Execution.Timing.Information.Disclosure` signature can't be filtered if *Application* is selected.

Bug ID	Description
489674	When scroll to the end of an muTable, GUI should shows 100% of entry.
489675	The Firefox web browser sometimes cannot delete performance SLA rules.
489715	Destination address should not be mandatory in GUI in *SD-WAN Rules*.
492898	Cannot delete FSSO AD group entries in GUI anymore.
493351	Object tooltip of last page should not always display on current page.
493773	SD-WAN rule in GUI unable to select (whether as source or destination) the address group `grp_citrixfarm`.
494724	When creating trunk interface on managed FSW, FSW ports in right-side list show down, even when some are up.
496613	Editing web filter profile in GUI deletes web-proxy profile and URL filter entries.
497667	FortiSwitch Ports page loads very slowly.
502785	Remove *# of interfaces* from device list.

HA

Bug ID	Description
408886	Uninterrupted upgrade from B718 to tag 9702 failed with 1.5M BGP routes and 6M sessions load.
461915	When `standalone config sync` is enabled in FGSP, IPv6 setting of interface is synced.
473806	Management interface IP address replicating to slave when using standalone management VDOMs.
473806	Management interface IP address replicating to slave when using standalone management VDOMs.
474622	`IPsec itn=0` after a unit joins an FGSP cluster.
482548	Conserve mode caused by `hasync` consuming most of memory.
485340	Cluster Uptime: -141 days -20:-31:-50.
486552	`vcluster` HA failover fails with large site-to-site IPsec VPN configuration on 3800D.
487444	FortiGate stops accepting traffic from any interface in a hardware switch after HA failover in 80/81E.
491311	Management port has sync'ed when creating a new NAT VDOM.
493759	When `vcluster2` is removed from HA config, all active sessions are killed once `session-ttl` is reached.
494029	After failover, sometimes cannot connect to *management-ip* of backup device.
501147	Moving VDOM to virtual cluster from GUI causes cluster to go out of sync.

IPS

Bug ID	Description
478185	Improve the ability of detection fragmented intrusion attacks.
489557	Strange traceroute issues when IPS is enabled.

IPsec VPN

Bug ID	Description
486756	Traffic is not fragmented for IPsec VPN when Proxy-based UTM is enabled.
489990	Make PKI validation of IDi & Certificate Identity optional.
490066	FortiClient with IPsec with Proxy / Webfilter - Fragmentation is needed.
491305	Packet from FortiClient cannot go through VXLAN over IPsec depending on packet size.
492046	FortiGate does not respond to INFORMATIONAL exchange message as requested by RFC.
493918	Memory leak with IKED.

Log & Report

Bug ID	Description
459306	Suggest to lower Threat Level for oversized file.
493140	Need to see application signature names instead of LDS under Logs & Report > System event logs.
494040	Creating or modifying security profiles generate multiple logs with misleading action.
497357	FortiGate logs show the action as block when we use DNS filter and if a DNS query timeout happens.
498519	Web filter authentication failed to set status field in the event log message.

Proxy

Bug ID	Description
479678	IPpool does not work properly in explicit Proxy-policy.
482916	WAD crashes with signal 6.
486821	Web application *Symphony* fails with AV profile enabled in policy.
487096	SSL handshake fails when activate ESET application.
491417	FortiGate is dropping server hello packets when URLFILTER is enabled.

Bug ID	Description
491424	Adjust the `proxy-auth-timeout` default value and unit.
491630	With UTM enabled, client failed to get response from server, gets 500 Internal error.
494081	WAD process crashes with signal 11 after upgrading the firmware to v5.6.4.

Router

Bug ID	Description
443948	High memory usage for `zebos_launcher` and `isisd`.
482631	OSPF adjacencies lost, FGFMD high CPU while pushing policies from FortiManager.
491423	BGP shutdown neighbor capability-default-originate parameter always in use.
491679	FortiGate chooses higher metric OSPF E2 route for traffic under some circumstance.
492063	Route map not able to set attribute with BGP conditional advertisement.
493454	Large PIM SM bootstrap packets are not forwarded with kernel 3.2.
494393	Router access list should not default to prefix any and exact match disable.
500673	SD-WAN rules with application do not work after HA switchover.

SSL VPN

Bug ID	Description
466438	High CPU usage by `sslvpnd`.
483712	`sslvpnd` consumes high memory causing FortiGate to enter conserve mode.
486918	SSL VPN web mode unable to load the page correctly.
489827	In SSL VPN web mode, `Visteon.service-now.com/vss` URL is not loading.
491895	Web mode SSL VPN HTTP bookmark not working.
494948	Confluence software is not rendered correctly in web mode.
494960	SSL VPN web mode has trouble loading internal web application.
494978	`authd` registers SSL VPN user with wrong user/group information and breaking SSL VPN after upgrade to 5.6.4.
498249	Need update SCEP over SSL host name/certificate check.
501769	SSL VPN: Bookmark to internal web site not loading correctly - JavaScript errors.

Switch

Bug ID	Description
493685	Hardware switch flooding traffic.

System

Bug ID	Description
370953	SLBC worker blade failed to re-synchronize with the config master blade due to the frozen confsync daemon.
394509	No log entry for failed admin PKI authentication.
414081	SMB1 support has been by default disabled under part models.
441483	Confused by `set enable-shaper disable` to enable HPE protection.
459273	Slave worker blade loses local administrator accounts.
462178	Front panel *SPEED* LED is flashing green when transmitting and receiving data.
466317	`[api]` is in Z state.
468938	Kernel panic on 3700D - slave.
472267	DNS filter performance improvement.
472270	SNMP feature for DNS filter counts.
473354	Suggest enable per-session-accounting on NP6Lite by default.
477886	PRP support.
479142	SLBC 5001D slave blade going out of sync.
481783	DHCP address assignment sometimes fails - DHCPD crashing multiple times.
485781	Deleting EMAC VLAN interface on a different VDOM causing connectivity loss to the EMAC VLAN for 5-7 pings.
493219	Softirq and nice are taking high CPU resources when sending and receiving packets with a virtual wire pair.
494603	FortiGate in transparent mode is not accessible over https/ssh (administrative access) once trusted host is configured.
494707	FortiGate `trusthost` settings not respected.
499332	No error message when configuring address `.067` and address converted with `.55`.
499435	Allow packet sniffer to use RAM disk.
499793	FortiGate set wrong timezone for Paraguay.

Upgrade

Bug ID	Description
495994	After upgrade to 5.4.9, observing a lot of IPS syntax errors on the console screen.

VM

Bug ID	Description
493225	FTG-VM01 is missing `diag sys mpstat` command option.
499154	FortiGate Azure rejects static route configure pushing from FortiManager.
501911	In FOS-AWS prompt, user password = instance ID, and force user to change password upon initial log in.

VoIP

Bug ID	Description
478634	Debug commands for SIP filter are not applied.

Web Filter

Bug ID	Description
454634	Web filter `set warning-prompt per-domain` is warning per-category instead of per-domain.
476806	FortiOS incorrectly sends ICMP "Destination Unreachable" with WF/certificate inspection.
486171	The *Web Rating Overrides* option doesn't work with flow-mode.
490377	The *Web Rating Overrides* option doesn't work properly on proxy-based.
498231	Web sites like *FedEx.com* is catogized as malicious category incorrectly.

Web Proxy

Bug ID	Description
500182	UDP over SOCKS proxy.

WiFi

Bug ID	Description
471638	FortiGate disconnects all clients when they roam from AP to AP.
479415	Incorrect `auth-success-page` *Authentication Success Page Replacement* message.

Bug ID	Description
491248	VAP RADIUS-based MAC authentication should support CoA.
491769	Support for third-party external portal with RADIUS MAC authentication.
495995	Custom categories override doesn't work.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
450553	FortiOS 6.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2017-12150 • CVE-2017-12151 • CVE-2017-12163
487421	FortiOS 6.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2018-13365
495090	FortiOS 6.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2018-13366
496431	FortiOS 6.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2018-9192
499552	FortiOS 6.0.2 is no longer vulnerable to the following CVE Reference: • CVE-2016-7431

Known Issues

The following issues have been identified in version 6.0.2. 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.

FortiGate 3815D

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

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	Using HA with FortiLink can encounter traffic loss during failover.
357360	DHCP snooping may not work on IPv6.

FortiView

Bug ID	Description
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
453610	*Fortiview->Policies(or Sources)->Now*, it shows nothing when filtered by physical interface at PPPoE mode.
460016	In *Fortiview* > *Threats*, drill down one level, click *Return* and the graph is cleared.
482045	FortiView – no data shown on *Traffic from WAN*.
494731	Incorrect reporting in Fortiview.

GUI

Bug ID	Description
256264	Realtime session list cannot show IPv6 session and related issues.

Bug ID	Description
439185	AV quarantine cannot be viewed and downloaded from detail panel when source is FortiAnalyzer.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
451776	Admin GUI has limit of 10 characters for OTP.
470589	The *Forward Traffic Log Details* panel *Security* tab does not display security log details when multiple log devices are enabled.
487350	*FortiGuard Filtering Services Availability* showing *Unavailable* on GUI when no valid Anti-spam license is present.
493839	Cannot change quota type (time-based, traffic-based).

HA

Bug ID	Description
451470	Unexpected performance reduction in case of Inter-Chassis HA fail-back with enabling HA override.
479987	FG MGMT1 does not authenticate Admin RADIUS users through primary unit (secondary unit works).
503433	`hasync` daemon crashes when admin session times out and cluster could be out of sync for a short period.

IPS

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 webfilter logs.

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.

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.
364280	User cannot use `ssh-dss` algorithm to login to FortiGate via SSH.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
440411	Monitor NP6 IPsec engine status.
466048	Huawei USB LTE E3276 cannot be detected.
468684	EHP drop improvement for units using `NP_SERVICE_MODULE`.
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.
482497	Running `diagnose npu np6lite session` in FGT-201E results in high CPU and system instability.
494042	If we create VLAN in VDOM A, then we cannot create ZONE name with the same VLAN name in VDOM B.

Upgrade

Bug ID	Description
470575	After upgrading from 5.6.3, `g-sniffer-profile` and `sniffer-profile` exist for IPS and webfilter.
473075	When upgrading, multicast policies are lost when there is a zone member as interface.

Bug ID	Description
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.

Web Filter

Bug ID	Description
480003	FortiGuard category does not work in NGFW mode policy.

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.