FortiOS - Release Notes

VERSION 5.2.5

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

February 16, 2017

FortiOS 5.2.5 Release Notes

01-525-301156-20170216

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-12-03	Initial release.
2015-12-07	Added FGT-VM64-AWS/FGT-VM64-AWSONDEMAND, build 8786, branch point 701 to Supported Models. Added 288299 to Resolved Issues. Added SSLVPN Web Mode: Windows 8/8.1 (32bit/62bit) IE 10, 11, Firefox 42 Mac OS 10.9 Safari
2015-12-09	Added 215890 to Known Issues.
2015-12-15	Added 218033 to Resolved Issues.
2015-12-17	Updated *Product Integration and Support > FortiAP support information*.
2016-01-12	Added 282154 to Resolved Issues. Added 306321 to Known Issues.
2016-01-14	Added 264674 to Resolved Issues.
2016-01-27	Added *Upgrade Information > FortiOS 5.2 Supported Upgrade Path* note.
2016-02-24	Added *Introduction > Last Release of Software* section.
2016-03-04	Added *Product Integration and Support > RHEL 7.1/Ubuntu 12.04 and later*.
2016-11-16	Added *Special Notices > Default DH-Param Change* section.
2017-02-16	Added 272927 to Resolved Issues and *Special Notices > Change default value for session-collector-interval*.

Introduction

This document provides the following information for FortiOS 5.2.5 build 0701:

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

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.2.5 supports the following models.

FortiGate	FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-SFP, FG-60C-POE, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FGT-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG- 111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG- 200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-310B-DC, FG-311B, FG-400D, FG-500D, FG-620B, FG-620B-DC, FG- 621B, FG-600C, FG-600D, FG-800C, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3000D, FG-3100D, FG-3016B, FG-3040B, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3950B, FG-3951B, FG-5001B, FG-5001C, FG-5001D, FG-5101C
FortiWiFi	FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-60D, FGR-100C
FortiGate VM	FG-VM32, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
FortiSwitch	FS-5203B
FortiOS Carrier	FCR-3810A, FCR-3950B, FCR-5001A-DW, and FCR-5001B FortiOS Carrier 5.2.5 images are delivered upon request and are not available on the customer support firmware download page. FortiOS Carrier firmware image file names begin with *FK*.

The following models are released on a special branch based off of FortiOS 5.2.5. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays the build number.

FGT-VM64-AWS	FGT-VM64-AWS is released on build 8786.
FGT-VM64-AWSONDEMAND	FGT-VM64-AWSONDEMAND is released on build 8786.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a **branch point field** that should read 0701.

The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0701-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0701-FORTINET.out image.

Last Release of Software

Due to the device flash size limitations, the following FortiGate models' last release of software will be FortiOS version 5.2.5. It is noted that these devices already have entered into their End-of-Life Cycle. Further details and exact dates can be found on the Fortinet Customer Support portal:

Affected Products:

- FortiGate FG-3016B
- FortiGate FG-3810A
- FortiGate FG-5001A SW & DW
- FortiCarrier FK-3810A
- FortiCarrier FK-5001A SW & DW

Special Notices

Compatibility with FortiOS versions

The following units have a new WiFi module built-in that is not compatible with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FWF-60CX-ADSL	PN: 8918-04 and later

The following units have a memory compatibility issue with FortiOS 5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Affected models

Model	Part Number
FG-600C	PN: 8908-08 and later
FG-600C-DC	PN: 10743-08 and later
FG-600C-LENC	PN: 11317-07 and later

Change default value for session-collector-interval

The default value for `session-collector-interval` changed from 8 to 64. Use the following command:

```
config system np6 set session-collector-interval 64
```

Router Prefix Sanity Check

Prior to FortiOS 5.2.4 under the config router prefix table, if there are any `le` and `ge` settings that have the same prefix length as the prefix, you may lose the prefix rule after upgrading to FortiOS 5.2.4 or later.

WAN Optimization in FortiOS 5.2.4

In FortiOS 5.2.4:

- If your FortiGate does not have a hard disk, WAN Optimization is not available.
- If your FortiGate has a hard disk, you can configure WAN Optimization from the CLI.
- If your FortiGate has two hard disks, you can configure WAN Optimization from the GUI.

See the FortiOS 5.2.4 Feature Platform Matrix to check the availability for your FortiGate model.

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.

Default DH Param Change

After 5.2.5, default `dh-params` increased from 1024 to 2048. If you want to use a lower `dh`, use the following CLI command:

```
config sys global
   set admin-ssh-v1 enable
end
```

FortiGate-92D High Availability in Interface Mode

The FortiGate-92D may fail to form an HA cluster and experience a spanning tree loop if it is configured with the following:

- operating in interface mode
- at least one of the interfaces, for example *interface9*, is used has the HA heartbeat interface
- a second interface is connected to an external switch

Workaround: use either WAN1 or WAN2 as the HA heartbeat device.

Default log setting change

For FG-5000 blades and FG-3900 series, log disk is disabled by default. It can only be enabled via CLI. For all 2U & 3U models (FG-3600/FG-3700/FG-3800), log disk is also disabled by default. For all 1U models and desktop models that supports STAT disk, log disk is enabled by default.

FG-5001D operating in FortiController or Dual FortiController mode

When upgrading a FG-5001D operating in FortiController or dual FortiController mode from version 5.0.7 (B4625) to FortiOS version 5.2.3, you may experience a back-plane interface connection issue. This is due to a change to the ELBC interface mapping ID. After the upgrade, you will need to perform a factory reset and then re-configure the device.

FortiGate units running 5.2.5

FortiGate units running 5.2.5 and managed by FortiManager 5.0.0 or 5.2.0 may report installation failures on newly created VDOMs, or after a factory reset of the FortiGate unit even after a retrieve and re-import policy.

FG-5001A and FG-3016B firmware image size

The FG-5001A and FG-3016B flash size used to store the firmware image and configuration files is reaching the limit. Fortinet recommends the following procedure to upgrade to 5.2.4 and later.

Example:

1. Backup the configuration in FortiOS 5.2.3.
2. Download FortiOS 5.2.4.
3. Format the flash.
4. Burn FortiOS 5.2.4 using TFTP from the BIOS.
5. Restore the configuration file.

Firewall services

Downgrading from 5.2.3 to 5.2.2 may cause the default protocol number in the firewall services to change. Double check your configuration after downgrading to 5.2.2.

FortiPresence

For FortiPresence users, it is recommended to change the FortiGate web administration TLS version in order to allow the connection.

```
config system global
   set admin-https-ssl-versions tlsv1-0 tlsv1-1 tlsv1-2
end
```

SSL VPN setting page

The default server certificate has been changed to the `Fortinet_Factory` option. This excludes FortiGate-VMs which remain at the `self-signed` option. For details on importing a CA signed certificate, please see the How to purchase and import a signed SSL certificate document.

Upgrade Information

Upgrading from FortiOS 5.2.3 or later

FortiOS version 5.2.5 officially supports upgrade from version 5.2.3 or later.

Upgrading from FortiOS 5.0.10 or later

FortiOS version 5.2.5 officially supports upgrade from version 5.0.10 or later.

When upgrading from releases prior to 5.0.11, if the source version is 5.0.10 with a configured HA cluster, you must schedule a down time; disable an uninterruptible upgrade; perform the upgrade; then, enable it back.

When upgrading from a firmware version beyond those mentioned in the Release Notes, a recommended guide for navigating the upgrade path can be found on the Fortinet documentation site.

There is separate version of the guide describing the safest upgrade path to the latest patch of each of the supported versions of the firmware. To upgrade to this build, go to FortiOS 5.2 Supported Upgrade Paths

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.

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 32-bit or 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 32-bit or 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 5.2.5 support

The following table lists 5.2.5 product integration and support information:

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 37 • Google Chrome version 43 • Apple Safari version 7.0 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Internet Explorer versions 8, 9, 10, and 11 • Mozilla Firefox version 27 • Apple Safari version 6.0 (For Mac OS X) • Google Chrome version 34 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	• 5.2.4 and later You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	• 5.2.0 and later • 5.0.7 and later You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• 5.2.5 and later
FortiClient iOS	• 5.2.2 and later
FortiClient Android and FortiClient VPN Android	• 5.2.6 and later

FortiAP	• 5.2.4 and later • 5.0.10 You should verify what the current recommended FortiAP version is for your FortiAP prior to upgrading the FortiAP units. You can do this by going to the *WiFi Controller* > *Managed Access Points* > *Managed FortiAP* page in the GUI. Under the *OS Version* column you will see a message reading *A recommended update is available* for any FortiAP that is running an earlier version than what is recommended.
FortiSwitch OS (FortiLink support)	• 3.3.0 and later Supported models: FSR112D-POE, FS108D-POE, FS224D-POE, FS124D, FS124D-POE, FS224D-FPOE • 3.2.0 and later Supported models: FS-108D-POE, FS-224D-POE, FSR-112D-POE • 3.0.1 and later Supported model: FS-224D-POE • 2.0.3 Supported models: FS-28C, FS-324B-POE, FS-348B, FS-448B
FortiSwitch-ATCA	• 5.0.3 and later Supported models: FS-5003A, FS-5003B
FortiController	• 5.2.0 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C • 5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• 2.1.0 • 1.4.0 and later • 1.3.0

Fortinet Single Sign-On (FSSO)	• 5.0 build 0242 (needed for FSSO agent support OU in group filters)
	  • Windows Server 2008 64-bit
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	• 4.3 build 0164 (contact Support for download)
	  • Microsoft Windows Server 2003 R2 (32-bit and 64-bit)
	  • Microsoft Windows Server 2008 (32-bit and 64-bit)
	  • Microsoft Windows Server 2008 R2 64-bit
	  • Microsoft Windows Server 2012 Standard Edition
	  • Microsoft Windows Server 2012 R2
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExplorer	• 2.7 build 1088 and later. Some FortiGate models may be supported on specific FortiExplorer versions.
FortiExplorer iOS	• 1.0.6 build 0130 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• 2.0.0 build 0003 • 1.0.0 build 0024
AV Engine	• 5.174
IPS Engine	• 3.086
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 and 6.0

Language support

The following table lists language support information.

Language support

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

Module support

FortiOS 5.2.5 supports Advanced Mezzanine Card (AMC), Fortinet Mezzanine Card (FMC), Rear Transition Module (RTM), and Fortinet Storage Module (FSM) removable modules. These modules are not hot swappable. The FortiGate unit must be turned off before a module is inserted or removed.

Supported modules and FortiGate models

Module	Type	FortiGate Model
ASM-S08	Storage	FG-310B, FG-620B, FG-621B, FG-3016B, FG-3810A, FG-5001A
FSM-064	Storage	FG-200B, FG-311B, FG-1240B, FG-3040B, FG-3140B, FG-3951B
ASM-FB4	Accelerated interface	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
ADM-XB2	Accelerated interface	FG-3810A, FG-5001A
ADM-FB8	Accelerated interface	FG-3810A, FG-5001A

Module	Type	FortiGate Model
ASM-FX2	Bypass	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
ASM-CX4	Bypass	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
ASM-CE4	Security processing	FG-1240B, FG-3810A, FG-3016B, FG-5001A
ADM-XE2	Security processing	FG-3810A, FG-5001A
ADM-XD4	Security processing	FG-3810A, FG-5001A
ADM-FE	Security processing	FG-3810A
RTM-XD2	Rear transition	FG-5001A
ASM-ET4	Security processing	FG-310B, FG-311B
RTM-XB2	Rear transition	FG-5001A
FMC-XG2	Security processing	FG-3950B, FG-3951B
FMC-XD2	Accelerated interface	FG-3950B, FG-3951B
FMC-F20	Accelerated interface	FG-3950B, FG-3951B
FMC-C20	Accelerated interface	FG-3950B, FG-3951B
FMC-XH0	Security processing	FG-3950B

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
Microsoft Windows XP SP3 (32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2323
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2323
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2323

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

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)	Microsoft Internet Explorer versions 9, 10 and 11 Mozilla Firefox version 33
Microsoft Windows 7 SP1 (64-bit)	Microsoft Internet Explorer versions 9, 10, and 11 Mozilla Firefox version 33
Microsoft Windows 8/8.1 (32bit/62bit)	Microsoft Internet Explorer versions 10 and 11 Mozilla Firefox 42
Mac OS 10.9	Safari 7
Linux CentOS version 5.6	Mozilla Firefox version 5.6
Linux Ubuntu version 12.0.4	Mozilla Firefox version 5.6

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 and 64-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 5.2.5. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Bug ID	Description
264674	Virus-infected files can not be quarantined when AV flow-based mode is enabled.

Device Visibility

Bug ID	Description
299500	Ensure Mac is not detected as an iPhone.

Firewall

Bug ID	Description
251549	Close LDAP connection when session times out in `fnbamd`.
282124	VSD crashes when `ssl-algorithm` custom is used.
294140	Proxyworker stops working on urlfilter response.
292734	Proxyworker ICAP memory issues.
279398	NP4 accelerated reused tcp session may be one-way accelerated or dropped
298937	`Proxyd ssl-exempt` must not check ip address if the hostname exists.
295017	`Authd fsso` client waits for the server hello indefinitely
269492	SIP SSL used the wrong CA when duplicate CAs were installed
282088	Radius Access-Request is missing from the `Calling-Station-Id` with wired 802.1X
286089	RSSO Endpoint attribute is overwritten with MAC address when client switches between SSIDs.
243964 280847 270229 279671	Move SSL traffic handling to proxyworker

Bug ID	Description
284655	Traffic blocked issue when `inspect_all` is enabled and no UTM profile is applied with NTurbo/IPS.
280440	GREv1 key is changed when crossing the FortiGate performing DNAT.
284891	When the VIP overlaps with the IPPool, that is not attached to the interface, the traffic to VIP is blocked by the Policy Check.
268626	Traffic is dropped when changing the working policy related configurations.
271151	Log message *Policy XX is too big for system, it's installed partially*. when saving a Policy.
292250	FortiClient is not able to get customized profile for policy based `ipsec vpn` of local user authentication

FortiGate-90D

Bug ID	Description
288299	Log disk missing after formatting the log disk and rebooting.

FortiGate 92D

Bug ID	Description
282629	Session cannot cross through FortiGate-92D VLAN interface.

FortiGate-1000D

Bug ID	Description
284929	NAT64 firewall blocks traffic when np6 offload is enabled.

FortiGate-3600C

Bug ID	Description
283044	PHY counters are missing.

FortiGate-5101C

Bug ID	Description
268727	After configuring `isf-acl`, the Kernel Panic Crash Log is displayed.

FortiGate-VM

Bug ID	Description
287875	Increase VM license expiration timeout and notice.

GUI

Bug ID	Description
280995	Certain address objects cause rendering issues on Internet Explorer.
287913	`js` error on firewall address because the list cannot be displayed in GUI
262009	GUI does not show the correct information about the actual DDNS configuration used.
276941	*No value* is returned when accessing Virtual Switch interface's OIDs.

High Availability

Bug ID	Description
286826	FortiGate does not send the certificate request when accessing via `ha-mgmt-interface`
268224	Email with a local report sent twice daily on FortiGate in HA mode.
285561	HA lost neighbour info and failover occurs after 497 days.
279280	`init_nids_db: ips_so_open failed, ret=-1` error messages on the console of the cluster slave.
288964	Debugzone mismatch keeps device out-of-sync even though all checksums are fully matched.
281439	FSSOD stops working on HA slave member.
283955	When HA failover occurs, the `bfd neighbor` disappears from the root VDOM.

IPS

Bug ID	Description
272927	The default value for `session-collector-interval` changed from 8 to 64. `config system np6 set session-collector-interval 64`.

IPsec

Bug ID	Description
286381 287534	IPSec:ESP packets are lost and duplicated after establishing the tunnel or rekey.

Log & Report

Bug ID	Description
257915	No traffic logs when related UTM log are generated.
266473	Add `policyid` field back for UTM logs.

Other

Bug ID	Description
218033	If the connection has been removed, the port still appears as connected.

Routing

Bug ID	Description
257798 260581 281357	Make the `ospf` interface config for template IPsec tunnel be applied to child interfaces.
267758	RADVD stops sending Router advertisements.

SSLVPN

Bug ID	Description
285406	Unable access FortiAnalyzer report via SSLVPN webmode.
287581	Hashtag is lost from the `href` when link is rewritten by SSLVPN.
286500	Cannot load `TLS1.X` website via SSLVPN webmode.
291009	SSLVPN causes high CPU spike.
292775	`SSLVPNd` may stop working with signal 11 in loop because of the IPv6 route.
284713	Remove the check of interface association in SSLVPN web portal address setting.

Spamfilter

Bug ID	Description
294401 291631	Not all email is detected as SPAM when using IMAP.

System

Bug ID	Description
294537	Correctly update DMAC when NTurbo is enabled and `ips_view_id` is greater than `0xfff` in NAT mode.
275897	The system up time's timer is not in sync with Netflow timer.
295724	Update Turkish daylight saving.
287438	VDOM verification failure issues on low-end FortiGate without VDOM support.
272927, 272089, 272927,218425	Improve NP6 SynProxy Monitoring.
281341	Remove/add port from the hardware switch, the LAN interface route missing.
293287	The DoS Policy(`tcp_syn_flood with syn-proxy`) protection is invalid when set to a low threshold.
288356	UDP/4500 packets are silently dropped by FortiGate on NP6 ports.
272395	When the IPS feature is enabled, the `icmp packet of ttl=1` passes through without the `ttl` decrement on FortiGate.
274258	Certificate output truncated.
284547, 284694	High CPU, NP6 counter drops and traffic loss.
287006	Cross-NP6 offloading does not work when destination interface is aggregated/LACP interface.
286847	VDOM verification does not work as expected on low-end FortiGates without VDOM support.
267790	Add drop counters for the NP6 port.
274250	DHCP6 Relay does not start after reboot.
278478	Change the loading mechanism of `AV-engine` and `AV-db`.
282694	NP6 drops an IPv6 packet with an unexpected next header.
282154	SDK support for 600C/800C/1000C .

Upgrade

Bug ID	Description
288707	`SSLVPN_TUNNEL_ADDR1` address object type changes after upgrading to 5.2.4.
287871	Administrative HTTPS and SSLVPN access using second WAN interface does not work as expected after upgrade to 5.2.4.

Wanopt & Webproxy

Bug ID	Description
288712	`www.europ-assistance.pt`, `www.europ-assistance.fr` is not accessible with explicit proxy and UTM.
292821	Improve HTTPS handling, cookie parsing and HTTP CONNECT processing.
288349	`ftp-over-http` does not work when IPS scan is enabled
285622	When using `wanopt` and `ssl-offloading` at the end of the `ssl-handshake`, WAD stops responding.

WiFi

Bug ID	Description
279136	Improve DARRP optimization algorithm.
267139	MAC address filtering stops in TP mode after reboot.

Known Issues

The following issues have been identified in version 5.2.5. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
260838	TCP flow may be incorrect and may be unable to support `AV fail-open` in flow mode.

Application Control

Bug ID	Description
273910	RTSP/RTP packets may not be forwarded if UTM (IPS and AppCtrl) is enabled.

FortiGate 3240C

Bug ID	Description
285520	TCP traffic may not be able to be offloaded in the decryption direction.

FortiGate 3700D

Bug ID	Description
279273	GRE tunnel on NPU VDOM link interface may not be able to pass traffic when off-load is enabled.

FortiGate 3810D

Bug ID	Description
285429	Traffic may not be able to go through the NPU VDOM link with traffic sharper enabled on FortiGate-3810D TP mode.

FortiGate-VM

Bug ID	Description
272438	During the boot-up sequence, the FortiGate-VM device may encounter a harmless configuration error message.

FortiSandbox

Bug ID	Description
269830	The UTM log may incorrectly report a file that has been sent to FortiSandbox. *FortiView* > *FortiSandbox* may still show files are submitted even after the daily upload quota has been reached.
273244	On the FortiGate device in *FortiView* > *FortiSandbox*, the analysis result may show a pending status and the FortiCloud side may show an unknown status.

FSSO

Bug ID	Description
285625	`SSO_Guest` users may not be able to pass FW after they agree to disclaimer.

GUI

Bug ID	Description
267957	The Top Interfering APs chart in the 5G Radio Spectrum Analysis Window may be empty.
268346	*All sessions: filter application*, *threat*, and *threat type*, may not work as expected
271113	When creating an `id_based policy` with SSL enabled, and the set `gui-multipleutm disable` is applied, an *Entry not found* error message may appear.
278638	Explicit policy may be automatically reset to log security events.
285813	When navigating `FortiView > Application` some security action filters may not work.
285831	In *FortiView* > *All Session* view, all entries may be displayed no matter which option is set on security action filter.
286226	Users may not be able to create new address objects from the Firewall Policy.
246546	Adding an override application signature may cause all category settings to be lost.
215890	Local-category status display may not change after running `unset category-override` in the CLI.

HA

Bug ID	Description
283697	When a new device joins, the list of devices may not synchronize between master and slave.

System

Bug ID	Description
285981	Adding more than eight members to `LACP get np6_lacp_add_slave` may result in an error.
263864	When the interface is configured with *Auto-Speed*, FG-3240C NP4 Port 1G may stay down after reboot. **Workaround**: Set the interface speed to *1000/Full*.
302272	Medium type may be shown incorrectly on shared ports.
306321	Interface may be mandatory for configuring the GRE tunnel.

VoIP

Bug ID	Description
272278	SIP calls may be denied when using a combination of SIP ALG, IPS, and AppCtrl.

Webfilter

Bug ID	Description
284661	If the requested URL has port number, the URL filter may not block properly.

WiFi

Bug ID	Description
267904	If the client is connecting to an SSID with WPA-Enterprise and User-group, it may not be able to pass the traffic 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.