FortiOS - Release Notes

VERSION 5.2.4

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

November 16, 2015

FortiOS 5.2.4 Release Notes

01-524-283783-20151116

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-07-22	Initial release.
2015-07-23	Bug 241646 added to Resolved Issues List.
2015-07-27	Bug 270217 added to Resolved Issues List.
2015-07-29	Added the following bugs to Resolved Issues List: 271256 272928 272929 263252 254815
2015-07-30	Bug 286595 added to Resolved Issues List.
2015-08-05	Bug 287871 added to Known Issues List. Updated the Upgrade Section with the following Note: Administrative access to the FortiGate using HTTPs and SSLVPN access with the second WAN interface may fail upon upgrading to 5.2.4. Added FG-VM64-SVM and FG-VM64-VMX build number 8542, branch point 688 to Supported Models.
2015-08-10	Added FG-400D build number 4972, branch point 688; and FG-600D, build number 4973, branch point to Supported Models.
2015-08-11	Added Built-In Certificate information to Special Notices. Bug 263864 added to Known Issues List.
2015-08-18	Added FG-3000D and FG-3100D build number 4991, branch point 688 to Supported Models.
2015-08-19	Added FG-5902D build number 4994, branch point 688 to Supported Models.
2015-08-28	Added FG-900D build number 5026, branch point 688 to Supported Models.
2015-09-02	FSSO 4.3 build 0164 contact Support for download.
2015-09-09	Added bug 246546 to Known Issues List.
2015-09-16	Added bug 284891 to Known Issues List.

Date	Change Description
2015-09-22	Added WAN Optimization Information to Special Notices.
2015-09-28	Added bug 268019 to Resolved Issues List.
2015-10-05	Added Prefix List Sanity Check Information to Special Notices
2015-10-13	Added FG-3200D: build number 5069, branch point 688 to Supported Models.
2015-10-26	Added 288707 to Known Issues List.
2015-10-27	Updated Upgrade Information. Added FK-3810A and FK-3950B to Supported Models List.
2015-10-28	Added 275832 to Resolved Issues List.
2015-11-09	Added FT-3815D: build 5098, branch point 688 to Supported Models.
2015-11-16	Updated Special Notices.
2016-01-12	Added 306321 to Known Issues List.
2016-03-04	Added RHEL 7.1/Ubuntu 12.04 and later to Product Integration and Support.

Introduction

This document provides the following information for FortiOS 5.2.4 build 0688:

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

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS 5.2.4 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-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-500D, FG-600C, FG-620B, FG-620B-DC, FG- 621B, FG-800C, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, 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, FCR-5001B, FK-3810A, and FK-3950B FortiOS Carrier 5.2.4 images are delivered upon request and are not available on the customer support firmware download page

The following models are released on a special branch based off of FortiOS 5.2.4. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays the build number.

FG-400D	FG-400D is released on build 4972.
FG-600D	FG-600D is released on build 4973.
FG-900D	FG-900D is released on build 5026.
FG-3000D	FG-3000D is released on build 4991.
FG-3100D	FG-3100D is released on build 4991.
FG-3200D	FG-3200D is released on build 5069.
FG-3815D	FG-3815D is released on build 5098.
FG-VM64-SVM **FG-VM64-VMX**	FG-VM64-SVM and FG-VM64-VMX is released on build 8542.
FT-5902D	FT-5902D is released on build 4994. FT-5902D is supported by the following FortiGate blade models, which require a special image: FG-5001D Please contact Fortinet Customer Support to download the image.

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 0688.

The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0688-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0688-FORTINET.out image.

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

Prefix Sanity Check prior to Upgrade

Starting in FortiOS 5.2.4, `le` or `ge`must be assigned values. Otherwise, the user will need to unset both `le` and `ge` prior to upgrade to ensure the prefix list rules are preserved.

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.

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 5.2.4

FortiGate units running 5.2.4 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:

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 5.2.1 or later

FortiOS version 5.2.4 officially supports upgrade from version 5.2.1 or later.

Upgrading from FortiOS 5.0.10 or later

FortiOS version 5.2.4 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.

Administrative access to the FortiGate using HTTPs and SSLVPN with the second WAN interface may fail upon upgrading to 5.2.4.

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 5.2.4 support

The following table lists 5.2.4 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	• 5.2.3 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	• 5.2.3 and later
FortiClient iOS	• 5.2.2 and later
FortiClient Android and FortiClient VPN Android	• 5.2.5 and later

FortiAP	• 5.2.4 and later • 5.0.9 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 0241 (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	• 2.6 build 1083 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	• 5.171
IPS Engine	• 3.079
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	Documentation
English	✔	✔
Chinese (Simplified)	✔	-
Chinese (Traditional)	✔	-
French	✔	-
Japanese	✔	-
Korean	✔	-
Portuguese (Brazil)	✔	-
Spanish (Spain)	✔	-

To change the FortiGate language setting, go to *System* > *Admin* > *Settings*, in *View Settings* > *Language* select the desired language from the drop-down menu.

Module support

FortiOS 5.2.4 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

Module	Type	FortiGate Model
ADM-XB2	Accelerated interface	FG-3810A, FG-5001A
ADM-FB8	Accelerated interface	FG-3810A, FG-5001A
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)	2317
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2317
Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)	2317

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
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	✔	

Product	Antivirus	Firewall
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 5.2.4. For inquires about a particular bug, please contact Customer Service & Support.

Antivirus

Bug ID	Description
272684	When sending a report to a FortiSandbox, increase the FortiGate support to up to 2K URL length.

Client Registration

Bug ID	Description
272115	After disabling `threat-weight`, Client Reputation information is still displayed in the UTM log.

Device Visibility

Bug ID	Description
278665	If `FCT-Access` is enabled on an interface, the FortiOS starts detecting and identifying devices.
279659	When the user changes *user device* and *device group*, and if they are referenced by the exempt list, update the `iprope`.
272928 272929	Improve the accuracy of device identification.

DLP

Bug ID	Description
261567	DLP sensor did not detect or scan malicious attachments in on-premises version of OWA.
271232	DLP PDF reader does not correctly identify font.

ELBC

Bug ID	Description
258155	`5203b Cluster` does not respond to the `SNMP gets/walks` for the `fgHaStats table`.
270267	A firewall node within a Standby ELBC sends logs as if it were processing packets.
280131	Content Cluster does not support `ipv6 load balancing`.

Firewall

Bug ID	Description
254815	IPv6 DoS Policies quarantining incorrect IPv6 addresses.
266939	If an `auth-login` is associated with a user but a group set is not matched, the kernel object `ip_user` is not released.
269863	The proxy bypasses the session if the response code is not 200.
270383	Status of the traffic log when using a secondary IP is incorrect.
271015	Diffie-Hellman prime sizes larger than 2048-bit in proxy SSL deep-inspection are not allowed.
273909	SSL offloading connection cannot be established.
274245	`fmbamd` does not match the correct tunnel peer group.
274735	If the `vdom config` is restored, the `iplist` is not updated properly.
274957	When the SSL Offload is full and combined with `http-multiplex` the virtual server stops working.
275216	`profile-protocol-options-oversize-log` controls the `uncompressed-size-limit logs`.
275261	After receiving a URL from ICAP, the Explicit Proxy sends an incorrect request.
275724	`full-mode` SSL offload to handle clients that offer TLS 1.2 as a record version is not enabled.
275729	Mobile IPv6 packets are not forwarded.
276206	`urlfilter` in the proxy does not handle URL patterns without a hostname
279693	`diag firewall statistic show` displays Global Statistics not per-VDOM stats.

FortiCarrier

Bug ID	Description
265846	Unable to downgrade or upgrade the FortiCarrier Platform.
277652	`diag firewall gtp [tunnelpath] list` causes high CPU usage.

FortiGate 92D

Bug ID	Description
273833	Passes STP BPDU between internal faces, which can cause a BPDU loop.

FortiGate 5001C

Bug ID	Description
271652	FGT-5001C blade stops passing traffic and randomly reboots.

FortiGate-VM

Bug ID	Description
265743	Increase the KVM interface number to 10.

FortiSandbox

Bug ID	Description
271256	Incorrect FortiSandbox status information displayed.

GUI

Bug ID	Description
269169	Users may not be able to create a site to site VPN with wizard using the PPoE Interface.
270342	When adding guest users, an error message should be displayed according to the CMDB error code.
271153	Reserved Cluster Management IP appears in all VDOMs.
272129	When the Source Address Filter contains a subnet, users cannot modify the VIP.
274872	`auto-asic-offload` is re-enabled automatically for any policy configuration change.

Bug ID	Description
275019	When editing interface settings, the admin assigned to the `prof_admin` profile returns `&quot_Permission_Denied&quot`.
275377	Secondary IP and netmask for VLAN interfaces may be reversed.
275547	Some certificates break the Certificates Page.
277858	When importing a GoDaddy CRL via HTTP, the Certificates page is blank.
268019	The VWL and link-monitor status is not correctly indicated in the GUI.

High Availability

Bug ID	Description
257197	HA Cluster slave unit does not disk log the `ftp upload`.
263737	`hasync` stops synchronizing the configuration due to the file descriptor being exhausted.
264371	HA failover time is not consistent.
267878	The `mtu` on the `port_ha` interface is not set properly.
268393	When there is a member change, `ha_ses_change_id()` is called and updates all of the sessions' timers.
271219	Set `diag sys ha set-as-master` to be hidden and add a warning for the `enable` command.
276779	Access to the `ha-mgmt-interface` cannot be controlled by `allowaccess setting` of the `ha-mgmt` interface.
279762	Duplicate MAC addresses occur when using virtual clusters on a platform with more than 32 ports.
280198	Prevent the NPU setting from making FortiGate 3700D slave box from rebooting.
281756	The expiration timer no longer updates after an HA failover in an AP cluster.

IPS

Bug ID	Description
270217	SNMP trap triggered when beta IPS signature is detected.
275832	Initialization bug in IPS daemon.

IPsec

Bug ID	Description
242425	After HA failover with multiple ISPs, FortiAnalyzer logging over IPsec stops working.
253746	IPsec failure message is not shown when a certificate is being listed in the CRL.
267889	After an IPsec re-key, the SCTP sessions are not correctly offloaded.
274557	Unable to establish IPsec VPN Tunnel from iOS device with a token.
279758	When reassembling fragmented IKE messages, memory leaks occur.

Log & Report

Bug ID	Description
247934	When FortiGate is connected FortiAnalyzer, email filter logs stored in the FortiAnalyzer are not displayed in the FortiGate GUI.
272702	`icmp` echo reply is incorrect in the IPS Security Log.
272970	IPS logs does not contain a hostname field.
279399	Traffic log columns are removed from list.
281526	In sniffer mode, unknown-0 interface field in traffic log appears.

Routing

Bug ID	Description
275016	Make the `vrrpd` bigger for the VRRP socket.
275894	After a network change, some OSPF LSA-Summary routes are not installed.
278350	Link monitor event log message is misleading.
278640	IGMP stops working when `warn_rlimt` timer times out.

SSL VPN

Bug ID	Description
258979	Client Certificate accepted even if the CRL is expired.
265524	SAP Portal does not work through SSL VPN Web Mode.

Bug ID	Description
269258	When accessing a specific tab in the bookmark page, the SSL VPN does not rewrite URL in GET request.
269758	SSL Web Mode portal does not load custom web page with the AJAX component.
269808	Web Application Combo Boxes and Date Pickers are not displayed properly via SSL VPN Web Mode.
270106	SSL VPN radius challenge user is not in the correct group if another user policy is used.
270260	SSL VPN Web Portal Bookmark does not return a complete HP Portal.
271190	SSL VPN Web Portal RDP Connector has a partial password leak.
271428	SSL VPN Web Mode cannot access the internal Open-XChange application.
271439	When a website is accessed through SSL VPN Web Mode Bookmark, file uploads do not work.
271791	SSL VPN stops working after reaching VDOM limit.
272628	Cannot access web site `ss.zhizhen.com`
272724	Unable to load `booking.hsmc.edu.hk` via SSL VPN Web Mode.
273112	Cannot access some web pages through SSL VPN Web Mode.
274260	OWA does not work properly by using SSL VPN with Web Portal mode.
274408	Handling of the JavaScript rewrite is not correct for certain files.
276480	SSL VPN Web Mode does not load the customized web page hosted on an internal web server.
279677	After setting TLS 1.0, the SSL proxy still uses TLS 1.2 in the client hello handshake.

System

Bug ID	Description
234009	Aggregate and redundant port member permutations are not handled correctly.
241646	Traffic cannot pass through the VLAN NP6 Interface based on a LAG TP VDOM.
251050	UML290 Modem loses connection after running for several days.
259515	NPU Offloading in TP VDOM stops forwarding traffic over to the IPsec VPN.

Bug ID	Description
263252	Improve handling of abnormal RSH packets and prevent system overflows and crashes.
264653	If there is a local LDAP user with a token, command: `diagnose test authserver ldap` displays a *Fail* status when it is successful.
267046	PPPoE does not negotiate after reboot.
267766	Fiber's link status changes after copper's link status changes.
268533	SCTP/GTP traffic is interrupted inside the IPsec tunnel on LAG ports cross NP6.
268654	`cmdbsvr heap corruption` occurs during bootup.
268705	When importing an outdated CRL, a log message should be entered.
268929	`miglogd` stops working due to alert mail.
269170	When a user tries to add an IP overlapping object, an incorrect warning message appears.
270667	Configuration of port-pair disappears after rebooting.
271398	VLAN interface MTU is reset to a physical interface.
272419	Unsolicited NA is not sent when the VDOM moves from one `vcluster` to another.
272639	DHCP does not release IP on VDOM `config restore`.
273363	Improvements in how gratuitous ARP packets are sent to update network devices when the MAC address of an aggregate or redundant interface changes.
273372	When the VDOM session limit is specified and an asymmetric routing is enabled, as soon as the limit is reached the firewall bypasses the non-matched traffic.
273713	LACP packet stops working when incoming CPU traffic is high and the HA failover starts bouncing.
274262	Certificate CA limit is not enforced.
274561	Webfiltering license information is not received from FortiManager after upgrading.
276191	Radius `auth` does not work. *Error sending radius request: Socket operation on non-socket* error message appears.
277825	If an action is not recommended and dangerous, a warning message should appear.
277939	ARP request sent even if there is a Static ARP entry.
279223	FortiGate stops working when `sflow` is enabled.

Bug ID	Description
281350	IPsec decryption found in the wrong slot after an index overflow. It causes the packet to be directed to the wrong VLAN interface after decryption.
283370	`get sys arp` command output is not correct.
286595	After rebooting, FortiGate-Wifi 20D/30D/40C loses part of its configuration.

Upgrade

Bug ID	Description
262460	When upgrading FortiGate 80 to 5.0.9, the device may not bootup.
274251	After upgrade, explicit proxy service is incorrectly created when using the GUI.
280498	Max Endpoint License issue after upgrading from 5.0.

VoIP

Bug ID	Description
269597	When using TLS enabled VoIP profiles, IMD stops working during a reconfiguration of a firewall policy.

Webfilter

Bug ID	Description
271145	Character encoding of banned words in logs.

Known Issues

The following issues have been identified in version 5.2.4. 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 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.

Firewall

Bug ID	Description

284891	If an IP address is assigned to a VIP and IP pool containing the same IP address, the VIP may be assigned to the interface on which the request originated.
	
	Workaround:
	
	1. If IPPool is not used, remove it.
	2. Specify arp-reply on IPPool.
	
	`config firewall ippool`
	`edit "10.100.10.100"`
	`set startip 10.100.10.100`
	`set endip 10.100.10.100`
	`set arp-intf "wan1" <-------`
	`next`
	`end`
	
	Disable arp-reply on IPPool.
	
	`config firewall ippool`
	`edit "10.100.10.100"`
	`set startip 10.100.10.100`
	`set endip 10.100.10.100`
	`set arp-reply disable <--------`
	`next`
	`end`

FortiGate 1000D

Bug ID	Description
284929	NAT64 firewall may block traffic when `np6` offload is enabled.

FortiGate 3240C

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

FortiGate 3600C

Bug ID	Description
28304	PHY counters may be missing.

FortiGate 3700DX

Bug ID	Description
279273	GRE tunnel on NPU VDOM link interface may not be able to pass traffic when offload 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 3810D TP mode.

FortiGate 5101C

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

FortiGate-VM

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

FortiManager

Bug ID	Description
271059	FortiGate units running 5.2.3 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.
286162	FortiManager may not be able to install an administrator with a global scope access profile.

FortiSandbox

Bug ID	Description
269830	The UTM log may incorrectly report a file has been sent to FortiSandbox. *FortiView* > *FortiSandbox* may still show files are submitted even after the daily upload quota has been reached.
270091	Some unsupported file types, such as JavaScript and shell script, may be dropped from being scanned by FortiSandbox.
270403	*FortiView* > *FortiSandbox* drill-down details may not be available on certain FortiSandbox detections.
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 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-multiple-utm 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.

Bug ID	Description
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.

HA

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

SSL VPN

Bug ID	Description
285406	Users may not be able to access FortiAnalyzer reports via SSL VPN webmode.

System

Bug ID	Description
272089	NP6 `syn-proxy` may still work after deleting the DoS policy.
282694	NP6 may drop an IPv6 packet with an unexpected next header.
285981	Adding more than 8 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. Work around: Set the interface speed to 1000/Full.
306321	Interface may be mandatory for configuring the GRE tunnel.

Upgrade

Bug ID	Description
287871	Administrative access to the FortiGate using HTTPs and SSLVPN access with the second WAN interface may fail upon upgrading to 5.2.4.
288707	`SSLVPN_TUNNEL_ADDR1` address object type may change after the upgrade to 5.2.4.

VoIP

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

Wan Optimization and WebProxy

Bug ID	Description
285622	When using `wanopt` and `ssl-offloading` at the end of the `ssl-handshake`, WAD may stop working.

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.