FortiOS v5.2.2
Release Notes

FortiOS v5.2.2 Release Notes

October 27, 2015

01-522-256781-20151027

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other resultsmay vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Document Library	docs.fortinet.com
Fortinet Video Libarary	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2014-11-18	Initial release.
2014-11-19	Minor document update.
2014-11-26	Minor document update.
2014-11-28	Updated FortiSwitch support information.
2014-12-02	Added 0262033 to known issues section.
2015-10-27	Updated Upgrade Information.

Introduction

This document provides the following information for FortiOS v5.2.2 build 0642:

- Supported models
- What's new in FortiOS v5.2.2
- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

See the Fortinet Document Library for FortiOS documentation.

Supported models

FortiOS v5.2.2 supports the following models.

Table 1: Supported 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-94D-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-1240B, FG-1500D, FG-3016B, FG-3040B, FG-3140B, FG-3240C, FG-3600C, FG-3700D, FG-3810A, FG-3950B, FG-3951B, FG-5001A, 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
FortiGate Rugged	FGR-60D, FGR-100C
FortiGate VM	FG-VM32, FG-VM64, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN
FortiSwitch	FS-5203B

The FG-60D-3G4G-VZW model uses the FGT_60D_MC-v5-build0642-FORTINET.out image. The FWF-60D-3G4G-VZW model uses the FWF_60D_MC-v5-build0642-FORTINET.out image.

What's new in FortiOS v5.2.2

For a list of new features and enhancements that have been made in FortiOS v5.2.2 see the *What's New for FortiOS 5.2* document available in the Fortinet Document Library.

AV Engine

- Added an option to disable the Win32 emulator in AV scanning to improve email server responsiveness.

Endpoint Control

- Added support for 32,000 plus FortiClient configuration distribution through Endpoint Control Network Access Control.

Firewall

- The `%%PROTOCOL%%` tag is now supported in replacement messages from the transparent proxy.
- Certificate chaining for certificate inspection mode.
- NTP source port translation for port values bigger than 1024.

FortiGate VM

- Integrated VMware Tools into FortiGate VM.

Log & Report

- Improved `msg` for the `perf-stats` log.
- Added log rate statistics to the *Dashboard* widget.

Routing

- Increased BGP Peers to 16,000 on enterprise models.

SSL VPN

- Added a pop-up message when the connection limit is exceeded.

System

- Added hardware switch feature and SPAN functionality to 30D, 60D, and 90D series. Moved PoE ports out of the internal switch to independent interfaces.
- CPU and memory performance statistics logging improvement.
- Added ZTE MF667 modem support.

Web-based Manager

- Update the session list as part of FortiView.
- Improvements to the firmware upgrade page.
- Added tooltips for application categories.
- Added a warning when using deep SSL inspection mode in policy/SSL profile pages.
- FortiView for System Events, Admin Access, and VPN Events.
- Improved FSSO group Web-based Manager page.
- RADIUS & TACACS+ list improvements.
- Restore feature store for 30D series models.
- Switch controller is hidden on 600C/800C/1000C series models.
- Improved the GTP session search.

WiFi

- Added broadcast/multicast suppression for local bridge mode SSID for different packet types.
- FortiCloud WiFi support.

Special Notices

FG-5001D operating in FortiController or Dual FortiController mode

When upgrading a FG-5001D operating in FortiController or dual FortiController mode from v5.0.7 (B4625) to FortiOS v5.2.2, 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.

Compatibility with FortiOS versions

The following units have memory compatibility issue with FortiOS v5.2.1 and lower. It is recommended to use FortiOS 5.2.2 and later for these units.

Table 2: Affected models

Model	Part Number
FWF-60CX-ADSL	PN: 8918-05 and later
FG-600C	PN: 8908-08 and later
FG-600C-DC	PN: 10743-08 and later
FG-600C-LENC	PN: 11317-07 and later

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
```

FortiCarrier

FortiCarrier images are delivered upon request and are not available in the Customer Service & Support firmware download page.

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.

Upgrade Information

Upgrading from FortiOS v5.2.0 or later

FortiOS v5.2.2 officially supports upgrade from v5.2.0 or later.

Upgrading from FortiOS 5.0.8 or later

FortiOS v5.2.2 officially supports upgrade from v5.0.8 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.

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 VM 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 v5.2.2 support

The following table lists v5.2.2 product integration and support information.

Table 3: FortiOS v5.2.2 support information

Web Browsers	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 33 • Google Chrome version 38 • 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	• v5.2.1 and later • v5.0.10 and later You should upgrade your FortiManager prior to upgrading the FortiGate.
FortiAnalyzer	• v5.2.0 and later • v5.0.7 and later You should upgrade your FortiAnalyzer prior to upgrading the FortiGate.
FortiClient Microsoft Windows and FortiClient Mac OS X	• v5.2.2 and later
FortiClient iOS	• v5.2.0 and later
FortiClient Android and FortiClient VPN Android	• v5.2.4 and later

Table 3: FortiOS v5.2.2 support information (continued)

FortiAP	• v5.2.2 and later • v5.0.8 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 Web-based Manager. 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)	• v3.0.1 and later Supported model: FS-224D-POE • v2.0.3 Supported models: FS-28C, FS-324B-POE, FS-348B, FS-448B
FortiSwitch-ATCA	• v5.0.3 and later Supported models: FS-5003A, FS-5003B
FortiController	• v5.2.0 Supported models: FCTL-5103B, FCTL-5903C • v5.0.3 and later Supported model: FCTL-5103B
FortiSandbox	• v1.4.2 • v1.4.0 and later • v1.3.0
Fortinet Single Sign-On (FSSO)	• v4.3 build 0160 The following operating systems are supported: • 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	• v2.6 build 1083 and later. Some FortiGate models may be supported on specific FortiExplorer versions.

Table 3: FortiOS v5.2.2 support information (continued)

FortiExplorer iOS	• v1.0.6 build 0130 and later Some FortiGate models may be supported on specific FortiExplorer iOS versions.
FortiExtender	• v2.0.0 build 0003 • v1.0.0 build 0024
AV Engine	• v5.159
IPS Engine	• v3.059
Virtualization Software	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• 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 and 5.5

Always review the Release Notes of the supported platform firmware version before upgrading your FortiGate device.

Language support

The following table lists language support information.

Table 4: Language support

Language	Web-based Manager	Documentation
English	✓	✓
Chinese (Simplified)	✓	-
Chinese (Traditional)	✓	-
French	✓	-
Japanese	✓	-
Korean	✓	-

Table 4: Language support (continued)

Language	Web-based Manager	Documentation
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 v5.2.2 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.

Table 5: Supported modules and FortiGate models

AMC/FMC/FSM/RTM Module	FortiGate Model
Module: ASM-S08 Type: Storage	FG-310B, FG-620B, FG-621B, FG-3016B, FG-3810A, FG-5001A
Module: FSM-064 Type: Storage	FG-200B, FG-311B, FG-1240B, FG-3040B, FG-3140B, FG-3951B
Module: ASM-FB4 Type: Accelerated interface	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Module: ADM-XB2 Type: Accelerated interface	FG-3810A, FG-5001A
Module: ADM-FB8 Type: Accelerated interface	FG-3810A, FG-5001A
Module: ASM-FX2 Type: Bypass	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Module: ASM-CX4 Type: Bypass	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Module: ASM-CE4 Type: Security processing	FG-1240B, FG-3810A, FG-3016B, FG-5001A
Module: ADM-XE2 Type: Security processing	FG-3810A, FG-5001A
Module: ADM-XD4 Type: Security processing	FG-3810A, FG-5001A
Module: ADM-FE8 Type: Security processing	FG-3810A
Module: RTM-XD2 Type: Rear transition	FG-5001A
Module: ASM-ET4 Type: Security processing	FG-310B, FG-311B
Module: RTM-XB2 Type: Rear transition	FG-5001A

Table 5: Supported modules and FortiGate models (continued)

Module: FMC-XG2 Type: Security processing	FG-3950B, FG-3951B
Module: FMC-XD2 Type: Accelerated interface	FG-3950B, FG-3951B
Module: FMC-F20 Type: Accelerated interface	FG-3950B, FG-3951B
Module: FMC-C20 Type: Accelerated interface	FG-3950B, FG-3951B
Module: FMC-XH0 Type: 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.

Table 6: Operating system and installers

Operating System	Installer
Microsoft Windows XP Service Pack 3(32-bit) Microsoft Windows 7 (32-bit & 64-bit) Microsoft Windows 8 (32-bit & 64-bit) Microsoft Windows 8.1 (32-bit & 64-bit)	2307
Linux CentOS 6.5 (32-bit & 64-bit) Linux Ubuntu 12.0.4 (32-bit & 64-bit)	2307
Virtual Desktop for Microsoft Windows 7 Service Pack 1 (32-bit)	2307

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.

Table 7: Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 32-bit SP1	Microsoft Internet Explorer versions 9, 10 and 11 Mozilla Firefox version 33
Microsoft Windows 7 64-bit SP1	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.

Table 8: Supported Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection v11	✓	✓
Kaspersky Antivirus 2009	✓	
McAfee Security Center v8.1	✓	✓
Trend Micro Internet Security Pro	✓	✓
F-Secure Internet Security 2009	✓	✓

Table 9: Supported 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	✓	✓

Table 9: Supported Windows 7 32-bit and 64-bit antivirus and firewall software (continued)

Product	Antivirus	Firewall
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 v5.2.2. For inquires about a particular bug, please contact Customer Service & Support.

Endpoint Control

Table 10: Resolved endpoint control issues

Bug ID	Description
0248014	FortiGate and FortiClient have a discrepancy in displaying their On-Net/Off-Net status.
0256732	Unexpected SSL connection shutdown from the client side causes the `fcnacd` daemon to consume CPU.

Firewall

Table 11: Resolved firewall issues

Bug ID	Description
0202686	Replacement message `%%PROTOCOL%%` tag is not expanded in replacement messages.
0235170	Self originating traffic should not use `identity-based-route`.
0246476	FGTServer Set-Cookie should not be added to a load-balance reply unless necessary.
0248419	FortiGate does not use the *User-Name* from the RADIUS response.
0249510	UDP VIP load balance session failover does not work.
0250583, 0252780	`scanunitd` and `proxyworker` daemon memory handling enhancement.
0251394, 0252331	Traffic that passes the FortiGate twice is blocked in transparent mode when UTM is enabled.
0252320	The wrong policy may be matched after the authenticated session becomes dirty.
0253540	The length validation code for the Indication IE in GTPv2 Modify Bearer Request is wrong, which causes packet drop.
0253592	FortiGate ignores the DENY policy when authentication portal is disabled.
0254363	When a login user logs out in the keepalive page, the relevant sessions are not deleted until the hard timeout. Traffic is still able to pass the FortiGate.
0254904	When using multiple one-to-one IPPools in policy, the same client can be mapped with several IPs belonging to different pools.

Table 11: Resolved firewall issues (continued)

Bug ID	Description
0255623	TNS sessions hang when a VIP is defined for a mapped IP address shorter than the external IP address.
0256488	The TCP session disconnected when a firewall policy is changed.
0257241	The SSL session unexpectedly terminates after client key exchange and a change cipher spec message is displayed when proxy mode is enabled.

FortiCarrier

Table 12: Resolved FortiCarrier issues

Bug ID	Description
0254230	GTP traffic count logs are generated on the slave unit.

FortiGate 3040B/3140B

Table 13: Resolved FortiGate 3040B/3140B issues

Bug ID	Description
0249749, 0258264	SGMII mode issue with interfaces.

FortiGate VM

Table 14: Resolved FortiGate VM issues

Bug ID	Description
0252306	FortiToken cannot be used for console login.
0259630	The option to enable VDOMs has been removed from the We-based Manager. The related CLI command has been hidden.

High Availability

Table 15: Resolved high availability issues

Bug ID	Description
0231555	Traffic stops when `load-balance-all` is enabled in active-active HA.

IPsec VPN

Table 16: Resolved IPsec VPN issues

Bug ID	Description
0247729	NAT IPsec traffic is not decrypted by NP4lite/SoC2.
0248504	Fragmentation behavior of the IPsec interface changes when a session is offloaded.
0251170	ESP replayed packets generated by the kernel issue fixed.
0251431	IKED crashes after VDOM deletion.
0253221	Added IPsec offload feature for NP6.
0253680	Packets are tunnelled twice (ESP in ESP) by NP6 when the IPsec tunnel is terminated on an npu-vlink interface.
0254898	An IPsec tunnel interface may not come up after the FortiGate unit reboots if the tunnel is using DHCP mode.
0256492	When IPsec interfaces belong to the same zone, all existing established IPsec SA are brought down with multiple configuration changes.

Log & Report

Table 17: Resolved log & report issues

Bug ID	Description
0247483	Logs are not sent to FortiCloud.
0250058	The command `execute log delete-old logs` does not work as expected.
0252125	Added MAC device information into the sniffer traffic log so that the Web-based Manager can display the device field.

Spam Filter

Table 18: Resolved spam filter issues

Bug ID	Description
0254508	Spam submission link is not added to email.
0255345	Added multi-part boundary to an email in the right place to avoid attachment breaking.
0257510	Added .asia as part of the URL so it can be recognized by spam filter.

SSL VPN

Table 19: Resolved SSL VPN issues

Bug ID	Description
0229536	Not able to access SAP server bookmarks via web mode.
0231666	Improved the submit button for editorial login page with SSO.
0231798	The PortForward connection tool should close the session as soon as it is closed by the backend server.
0244399	Unable to handle remote web server return JavaScript as plain text type.
0251595	Unable to perform a OCSP CRL check properly.
0252113	The username is incomplete when using user certificate authentication.
0252337	No connection could be made when SSL VPN enter conserve mode.
0256000	Personal bookmarks of PKI users are not displayed in the web portal when the user logs in again.
0259136	SSL proxy can only use SSLv3 for the server side connection. TLS should be supported for the backend connection.

System

Table 20: Resolved system issues

Bug ID	Description
0226128	Improved DNS server query algorithm.
0244082	To ensure nturbo works as expected, traffic should not be offloaded to NPU if there is an interface-based policy enabled.
0246224	SCTP traffic cannot be offloaded on NP6.
0246849	Added a CLI command to control if a CR is sent after a connection is established.
0247062	FortiGate fails to update generic DDNS record when zone information is present in the server response.
0250439	After performing `factoryreset2`, the IPv6 default route is removed.
0250534	Adding or unsetting a member of an aggregation interface can cause the peer switch's interface to be down.
0251221	The hardware switch span port does not work on FG-200D-POE and FG-240D-POE models.
0251269	SNMP query for `entLogicalTAddress` is incorrect.
0252333	XLR crash when packets with priority bits are set in the VLAN tag.

Table 20: Resolved system issues (continued)

Bug ID	Description
0252947	With a FortiGate previously registered to both FortiManager and FortiCloud, it will still send management traffic to FortiManager even after it is unregistered from the FortiManager.
0253694	Resolved `radiusd` daemon memory issue caused by HA sync.
0253970	Long reboot time on a device with large configuration.
0254865	`get system source-ip status` does not scan LDAP server in VDOMs to report the `source-ip` manual setting.
0256486	ADSL is unable to connect after upgrading to v5.2.1.
0256491	Memory corruption in IPSA driver can cause system freeze condition.
0256498	Improved on how firewall policies are purged.
0256727	`cmdbsvr` crash after restoring a large configuration file without entering the VDOM licence.
0256730	Changed the default digest method from SHA to SHA256 for certificate request generation.
0257277	After deleting a VDOM, error messages are displayed when executing `get sys ha-nonsync-csum`.
0257341	Configuration restore does not restore the local certificate.
0257343	Updated Israel's Daylight Savings Time rules.
0258251	Sessions are dropped when a VLAN interface description is changed.
0258356	Failed to upload VDOM logs on vcluster2 to FortiAnalyzer.
0260730	The maximum files submitted to FortiCloud Sandbox should be enforced.

VoIP

Table 21: Resolved VoIP issues

Bug ID	Description
0233723	Removed port translation in the `LocationConfirm` packet when doing NAT for H.225.

WAN Optimization and Web Proxy

Table 22: Resolved WAN optimization and web proxy issues

Bug ID	Description
0253682	Improved WAN optimization HTTP 304 response processing in order to have the state synchronize properly.
0254020	Web proxy fails to connect server if the outgoing IP is configured.

Table 22: Resolved WAN optimization and web proxy issues (continued)

Bug ID	Description
0255010	Web proxy and session based authentication does not work for HTTP traffic when an ICAP profile is selected in policy.
0256228	WAN optimization is not available in policy when `srcintf` is `ssl.vdom`.
0259651	Memory leak in WAD worker process.

Web-based Manager

Table 23: Resolved Web-based Manager issues

Bug ID	Description
0193650, 0257997	Added an option to control the TLS and SSL versions for web administration.
0231693	Imported local certificate overrides previously imported certificate.
0235296	An *Internal Server Error 500* is encountered when the group address is edited.
0243143	Insert policy below/above is not adding a global-label to the new entry.
0245175	Improved SSL VPN configuration page.
0248270	Added icon and tool tips for oversized policy.
0249031	Configured VPN comments are displayed in VPN monitor.
0249121	An *Internal Server Error* on SSL VPN page is displayed when changing *sslvpn_tunnel_addr1* type to *subnet*.
0253573	Unable to properly create a new remote user group using the local user creation wizard due to a missing *OK* button.
0253649	Certain specific configurations can lead to VLANs being hidden from the VDOM interface list.
0254300	The FortiSwitch 5203B label is FortiGate 5203B in the main header.
0254301	The FortiGate Rugged 100C label is FortiGate 100C in the main header.
0257121	An *Internal Server Error* is displayed when accessing the Guest Management page.

Web Filter

Table 24: Resolved web filter issues

Bug ID	Description
0255209	In transparent mode, if Web Filter FortiGuard categories have the action set to *Warning*, the client's connection is reset and unable to reach the requested URL.

Known Issues

The following issues have been identified in v5.2.2. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Firewall

Table 25: Known firewall issues

Bug ID	Description
0253505	Changing the `dedicated-management-cpu` configuration may cause the unit to operate in an unstable state. Workaround: Reboot the device after changing the CPU configuration. Affected model: FG-3700D
0254210	Failed to block an EICAR sample on SMB 1.0 and 2.0 protocol when nturbo is enabled.

IPsec VPN

Table 26: Known IPsec VPN issues

Bug ID	Description
0253651	FortiClient may encounter an IPsec traffic issue with a FortiGate that has NP6 NPU offload enabled.

Log & Report

Table 27: Known log & report issues

Bug ID	Description
0260101	The log loss rate to FortiAnalyzer is higher than on previous builds.

Routing

Table 28: Known routing issues

Bug ID	Description
0262033	The VRRP status should not flap when the VRDST is unreachable.

System

Table 29: Known system issues

Bug ID	Description
0241646	Traffic may not go through VLAN interfaces based on LAG in transparent VDOMs. Workaround: After finish the configuration, perform a reboot operation.

0243840	In order to acquire FortiCloud services from FortiManager, you need disable default servers using the following command:
	`config system central management`
	`  set include-default-servers disable`
	`end`

0246126	IPv4 multicast traffic over an IPsec interface cannot be offloaded to NP6.
0253641	The `inbandwidth` limit does not work on NP6 interfaces.
0257807	The default UDP custom service has `tcp-portrange 0:0` in the configuration.
0257860	Software switch hub mode is not processing traffic properly.
0257874	The `diagnose npu np6 debug` CLI command can cause kernel debug message appear.
0259448	The `hardware-switch` setting is not enable by default for FGR-60D and FWF-60D-3G4G-VZW models.
0260799	XLP unable to process TCP traffic when fail-over occurs on an aggregate interface.

Upgrade

Table 30: Known upgrade issues

Bug ID	Description
0251511	Upgrades to v5.2.1 will encounter a configuration error with the antivirus service and HTTPS/FTPS/POP3S/IMAPS/SMTPS protocols because such configurations do not exist in `profile-protocol-options`.
0255603	Remove the default profile in `deep-inspection-option / ssl-ssh-profile` if it is not used. Otherwise, it will be renamed to `deep-inspection-5-0`.

Web-based Manager

Table 31: Known Web-based Manager issues

Bug ID	Description
0256449	The FortiAP *Recommended Update* does not support FAP-221C and FAP-320C models.
0257596	Flow based UTM profiles are not hidden in the explicit policy configuration page.
0258905	System event log column settings have duplicate and missing fields.
0260481	FortiView events may not be displayed due to timing issue caused by conflicts between the local PC and FortiGate time setting.
0260594	The IPv6 policy configuration page does not display the IPv6 address group.
0260711	A chart in the Cloud Application drill down tab for the 5 minute time period is empty.
0260754	An administrator that only has permission for Policy, Address, Service and Schedule configuration is unable to load the web pages related to those configuration objects.
0260795	FortiView may not display data due to the report database being unavailable.
0261864	Missing dependency checks for FortiView including report database and the new System, VPN, and Admin pages.

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.