FortiOS v5.0 Patch Release 5
Release Notes

FortiOS v5.0 Patch Release 5 Release Notes

April 11, 2014

01-505-220145-20140411

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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 Library	video.fortinet.com
Knowledge Base	kb.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
April 11, 2014	Added FG-VM64-AWS to "FortiGate VM" on page 9.
April 11, 2014	Added the FortiGate-60D-POE and FortiWiFi-60D-POE to "Supported models" on page 8. Removed references to FortiGate VMs from "New FortiOS Carrier features" on page 12.
March 17, 2014	Added more information to the description of the dedicated management CPU feature described in "System" on page 10. Added new resolved issues section: "Performance" on page 45.
February 24, 2014	New FortiAP-221C and 320C models supported. See "FortiAP support" on page 33. Add the FortiGate-70D to "Supported models" on page 8.
February 5, 2014	Re-wrote the following two sections so that they are the same for FortiOS Release 5.0 Patches 4, 5 and 6: • "Disk logging disabled by default on some models (Log to FortiCloud instead)" on page 15 • "FG-60D/FWF-60D logging to disk" on page 16
January 13, 2014	• Added "Upgrading an HA cluster" on page 20 • Added "Zone-related policies may be deleted when upgrading to FortiOS v5.0 Patch Release 4 or 5" on page 20 • Added a new feature to "System" on page 10: the Threat History widget has replaced the Reputation Score monitor used for Client Reputation, which has been removed.
December 31, 2013	• Added FG-1500D and FG-3700D to "Supported models" on page 8. • Added "FG-1500D and FG-3700D" on page 52 to "Known Issues" on page 52.
December 18, 2013	Added more information about threat history widget and client reputation changes to "Logging & Report" on page 10.
November 27, 2013	Added new section: "FortiCarrier" on page 9 to "Supported models" on page 8. Added new section: "New FortiOS Carrier features" on page 12. Corrected some of the entries in "SSL VPN standalone client" on page 37. Added resolved issue "0217408" on page 46.

Date	Change Description
November 12, 2013	Added the FortiGate-90D-POE and FortiWiFi-90D-POE to "Supported models" on page 8. Changes to "Special Notices" on page 12: • Changes to "Disk logging disabled by default on some models (Log to FortiCloud instead)" on page 15 • The section "Limiting access for unauthenticated users" on page 17 is a re-write of the former "ID-based firewall policy" section. Changes to "Upgrade Information" on page 20: • Added the section "DHCP sever reserved IP/MAC address list" on page 25. Changes to "Known Issues" on page 52: • Improved the information for issue "0212959" on page 55 • New section "Wireless" on page 55 describes issue "0219352" on page 54 Updated the supported operating systems in "SSL VPN standalone client" on page 37. Changes to "Resolved Issues" on page 39: • Updated issue "0213274" on page 47
November 1, 2013	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instruction to upgrade your device to FortiOS v5.0 Patch Release 5 build 0252. Please review all sections in this document prior to upgrading your device. For more information on upgrading your FortiOS device, see the *FortiOS 5.0 Handbook* at http://docs.fortinet.com.

This document includes the following sections:

Supported models

The following models are supported on FortiOS v5.0 Patch Release 5.

FortiGate

FG-20C, FG-20C-ADSL-A, FG-30D, FG-40C, FG-60C, FG-60C-POE, FG-60D, FG-60D-POE, FG-80C, FG-80CM, FG-90D, FGT-90D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-240D, FG-280D-POE, FG-300C, FG-310B, FG-310B-DC, FG-311B, 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, and FG-5101C.

FG-60D-POE and FWF-60D-POE

These models are released on a special branch based off of FortiOS v5.0 Patch Release 5. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4377` as the build number.

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 `252`.

FG-90D-POE and FWF-90D-POE

These models are released on a special branch based off of FortiOS v5.0 Patch Release 5. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4347` as the build number.

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 `0252`.

FG-70D

This model is released on a special branch based off of FortiOS v5.0 Patch Release 5. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4399` as the build number.

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 `0252`.

FortiGate Rugged

FGR-100C

FortiWiFi

FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, and FWF-90D-POE.

FortiGate VM

FG-VM32, FG-VM64, FG-VM64-AWS, FG-VM64-XEN, FG-VM64-KVM, and FG-VM64-HV

FG-VM64-AWS

This model is released on a special branch based off of FortiOS v5.0 Patch Release 5. As such, the *System* > *Dashboard* > *Status* page and the output from the `get system status` CLI command displays `4348` as the build number.

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 `252`.

FortiSwitch

FS-5203B

FortiCarrier

FCR-3810A, FCR-3950B, FCR-5001A-DW, and FCR-5001B

FortiOS v5.0 Patch Release 5 FortiCarrier images are delivered upon request and are not available on the customer support firmware download page. See “Upgrading older FortiCarrier specific hardware” on page 12

Summary of enhancements

The following is a list of enhancements in FortiOS v5.0 Patch Release 5 build 0252. For more information about new features in FortiOS v5.0 Patch Release 5 see Whats New in FortiOS 5.0.

Not all features/enhancements listed below are supported on all models.

Firewall

- Port block allocation used for Carrier Grade NAT (CGN) to reduce the logs generated by NAT
- FortiGate units can now preserve the value of the Class of Service (CoS) bit, also called Priority Code Point (PCP), when a packet traverses the FortiGate unit with virus scanning enabled.

Logging & Report

- Replace user names with ***anonymous*** in log messages (log anonymizing)
- Dashboard Traffic and Threat History widget drill down improvements. For example, the Threat History widget has replaced the Client Reputation Score monitor, which has been removed.

Routing

- Manually configure IPv6 neighbor cache entries

SSLVPN

- New SSL VPN portal history widget that shows log in history

System

- All FortiGate passwords can now be up to 128 characters
- Add Integrated switch fabric (ISF) access control list (ACL) short-cut path to FortiGate models FG-3240C, FG-3600C and FG-5001C.
- Dedicated management CPU: configure FortiGate models 1000 and above to dedicate CPU 0 for management. This means you can access the GUI or CLI and perform management tasks even with the system is very busy. Use the following command to dedicate CPU 0 for management-related processes:

```
config system npu
   set dedicated-management-cpu enable
end
```

- New ipmc_sensord daemon that handles all IPMC requests
- Switch controller added to new FortiGate models FG-200D, FG-240D, FG-280D-POE, FG-600C, FG-800C, and FG-1000C. This feature is used to manage FortiSwitch secure access switch models such as the FS-28C, FS-324B, and FS-348B.
- Support low level formatting of the FortiGate boot device and all hard disks using the `execute erase-disk` command.
- Support VLAN interface accounting feature of NP4
- FortiSwitch controller supports 2 uplinks for FS-348B and FS-448B
- Enable explicit proxy GUI for FortiGate working with FortiController
- Entropy token support for DRBG (deterministic random generator). You can enable or disable a FortiGate unit to used a USB entropy token when one is connected to a FortiGate USB port.
- PoE status displayed on the Unit Operation dashboard widget.
- The Threat History widget has replaced the Reputation Score monitor used for Client Reputation, which has been removed.
- Support added for NIST SP 800-135 KDF test vectors (for FIPS certification)
- Removed Object Tagging from the GUI

User authentication

- When configuring a user group, you can add an LDAP server, then browse the server user group you can browse LDAP servers and add selected user groups from the LDAP server.
- Endpoint control GUI page moved to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.

Wireless

- FAP-11C, FAP-14C and FAP-28C LAN port support - The Ethernet LAN ports on these devices can be connected to an Ethernet network. Wired clients connected to this Ethernet network can communicate through the FortiAP to the FortiGate unit that is controlling the FortiAP. Wired client traffic can be merged with or kept separate from the SSIDs on the FortiAP device.
- Options to improve performance by preventing packet fragmentation of CAPWAP traffic between the FortiAP and the FortiGate unit. You can:
  - Set the MTU size of uplink and downlink CAPWAP packets,
  - Configure the FortiAP to adjust the Maximum Segment Size (MSS) of TCP packets sent by wireless clients
  - Cause the FortiAP unit to block TCP and UDP packets that are too large and would cause packet fragmentation.
- Presence detection (also called station-locate) feature to FortiWiFi units. This feature, already added to FortiAP units, allows FortiWiFi units to detect and record info about wireless devices that do not specifically connect to the FortiWiFi wireless network.
- JSON reset command to reset presence detection
- FortiAP units can be authorized (pre-authorized) with a FortiGate unit without connecting to it
- Support max-distance between FortiGate and FortiAP

Special Notices

New FortiOS Carrier features

Changes to licensing

Prior to FortiOS 5.0, only FortiCarrier-specific hardware could run FortiOS Carrier 4.0. Starting with FortiOS 5.0.2, the FortiOS Carrier Upgrade License can be applied to selected FortiGate models to activate FortiOS Carrier features. There is no support for FortiOS Carrier features in FortiOS 5.0 GA and 5.0 Patch Release 1.

At this time the FortiOS Carrier Upgrade License is supported by FortiGate models FG-3240C, FG-3950B, FG-5001B, FG-5001C, and FG-5101C. Future 3000 and 5000 series models are also expected to support FortiOS Carrier.

You can obtain a FortiOS Carrier license from your Fortinet distributor. On a FortiGate model that supports FortiOS Carrier and that is running FortiOS 5.0 Patch Release 2 or later you can use the following command to activate FortiOS Carrier features:

```
execute forticarrier-license <license-key>
```

The license key is case-sensitive and includes dashes. When you enter this command, FortiOS attempts to verify the license with the FortiGuard network. Once the license is verified the FortiGate unit reboots. When it restarts it will be running FortiOS Carrier with a factory default configuration.

You can also request that Fortinet apply the FortiOS Carrier Upgrade license prior to shipping a new unit, as part of Professional Services. The new unit will arrive with the applied license included.

Licensing and RMAs

When you RMA a FortiGate unit that is licensed for FortiOS Carrier, make sure that the FortiCare support representative handling the RMA knows about the FortiOS Carrier license. This way a new FortiOS Carrier license will be provided with the replacement unit.

Licensing and firmware upgrades, downgrades and resetting to factory defaults

After a firmware upgrade from FortiOS 5.0 Patch Release 2 or later you should not have to re-apply the FortiOS Carrier license. However, the FortiOS Carrier license may be lost after a firmware downgrade or after resetting to factory defaults. If this happens, use the same command to re-apply the FortiOS Carrier license. FortiGuard will re-verify the license key and re-validate the license.

Upgrading older FortiCarrier specific hardware

Previous versions of FortiOS Carrier run on FortiCarrier specific hardware. This includes FCR-3810A, FCR-3950B, FCR-5001A-DW, and FCR-5001B.

As long as the FortiCarrier hardware can be upgraded to FortiOS 5.0.2 or later, it can be upgraded to FortiOS Carrier 5.0.2 or later without purchasing a new FortiOS Carrier Upgrade License. You must use FortiCarrier firmware to upgrade this hardware and this firmware may not be available from the Fortinet Support Site. Please work with your Fortinet representative to ensure a smooth upgrade of these FortiCarrier models.

Changes to GPRS Tunneling Protocol (GTP) support

FortiOS Carrier 5.0 supports GTP-C v2, which is the control plane messaging protocol used over 4G-LTE 3GPP R8 software interfaces, as well as between LTE networks and older 2G/3G networks with general packet radio service (GPRS) cores.

Changes to MMS scanning

MMS scanning now includes data leak prevention (DLP) to detect fingerprinted and/or watermarked files transferred via MMS, as well as data pattern matching for data such as credit cards and social security numbers.

SCTP firewall support

LTE networks require support for the SCTP protocol to transfer control plane data between evolved NodeBs (eNBs) and the Mobility Management Entity (MME), as well as between the MME and the Home Subscriber Server (HSS). SCTP firewall support is included in FortiOS 5.0 and FortiOS Carrier 5.0. SCTP traffic is accepted by FortiOS Carrier and you can create SCTP services and security policies that use these services. All other security feature can also be added as required to security policies for SCTP services.

TFTP boot process

The TFTP boot process erases all current firewall configuration and replaces it with the factory default settings.

Monitor settings for Web-based Manager access

Fortinet recommends setting your monitor to a screen resolution of 1280x1024. This allows for all the objects in the Web-based Manager to be viewed properly.

Before any upgrade

Upgrade your FortiOS device during a maintenance window. To minimize any adverse impact your users and your network, plan the firmware upgrade during a maintenance window. This allows you to properly upgrade, test, and implement the firmware upgrade.

Save a copy of your FortiGate configuration prior to upgrading. To backup your FortiGate configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration* and save the configuration file to your local hard drive.

In VMware environments, it is recommended that you take a *Snapshot* of the VM instance prior to upgrading. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

In Citrix XenServer environments, it is recommended that you take a Snapshot of the VM instance prior to upgrading. In the event of an issue with the firmware upgrade, use *Virtual Machines Snapshots* to revert to the *Snapshot*. To create a Snapshot, right-click the VM instance and select *Take a Snapshot*.

Open Source Xen does not natively support *Snapshots*. You can create a backup of LVM partitions with the *LVM Snapshots* feature and then restore this backup. You can also use Linux commands to backup and restore a virtual machine.

After any upgrade

If you are using the Web-based Manager, clear your browser cache prior to login on the FortiGate to ensure the Web-based Manager screens are displayed properly.

The AV and IPS engine and definitions included with a firmware upgrade may be older than ones currently available from the FortiGuard Distribution Server (FDS). Fortinet recommends performing an *Update Now* after upgrading. Go to *System* > *Config* > *FortiGuard,* select the blue triangle next to *AV & IPS Download Options* to reveal the menu, and select the *Update Now* button. Consult the *FortiOS v5.0 Handbook* for detailed procedures.

Using wildcard characters when filtering log messages

While using filtering in the log message viewer you may need to add * wildcard characters to get the search results that you expect. For example, if you go to *Log & Report* > *Event Log* > *System* to view all messages with the word “logged” in them you can select the Filter icon for the *Message* list and enter the following:

logged

Including both * wildcard characters will find all messages with “logged” in them. “logged” can be at the start or the end of the message or inside the message.

If you only want to find messages that begin with the search term you should remove the leading *. If you only want to find messages that end with the search term you need to remove the trailing *.

It does not work to add a * wildcard character inside the search term. So searching for *lo*ed* will not return any results.

Default setting/CLI changes/Max values changes

- The number of firewall address groups has been increased to 20,000
- The number of addresses in a firewall address group has been increased to 1000
- The number of Static IP/MAC bindings has been increased
- The number of SSL VPN portals has been added to the maximum values document
- The number of SSL VPN portals has been increased to 10 for the FortiGate models FG-60D, FG-80, and FG-90D.

IPS algorithms

For optimal performance on your FortiGate unit, the IPS algorithm can be configured via the CLI. Select one of the following modes:

- engine-pick: The IPS engine picks the best algorithm to use.
- high: This algorithm fits most FortiGate models
- low: This algorithm works best on FortiGate units with less memory (512 MB or less)
- super: This algorithm works best on FortiGate models with more memory (more than 4 GB)

To configure the algorithm, use the following CLI commands:

```
config ips global
  set algorithm [engine-pick | high | low | super]
end
```

Disk logging disabled by default on some models (Log to FortiCloud instead)

For the following FortiGate and FortiWiFi models, disk logging is disabled by default and Fortinet recommends logging to FortiCloud instead of logging to disk:

- FG-20C, FWF-20C
- FG-20C-ADSL-A, FWF-20C-ADSL-A
- FG-40C, FWF-40C
- FG-60C, FWF-60C, FG-60C-POE, FWF-60CM, FWF-60CX-ADSL-A
- FG-60D, FWF-60D, FG-60D-POE, FWF-60DM, FWF-60DX-ADSL-A
- FG-80C, FWF-80C, FG-80CM, FWF-80CM
- FG-100D (PN: P09340-04 or earlier)
- FG-300C (PN: P09616-04 or earlier)
- FG-200B/200B-PoE (if flash is used as storage)

If you were logging to FortiCloud prior to upgrading to FortiOS v5.0 Patch Release 5, the settings are retained and logging to FortiCloud continues to operate normally. If you were logging to disk prior to upgrading, logging to disk may be disabled during the upgrade process.

If required, you can enable disk logging from the CLI using the following command:

```
config log disk setting
  set status enable
end
```

If you enable disk logging on the models listed above, the CLI displays a message reminding you that enabling disk logging impacts overall performance and reduces the lifetime of the unit.

A code limitation specific to the FG-80C, FG-80CM, FWF-80C, and FWF-80CM models prevents the warning message from being displayed.

FG-60D/FWF-60D logging to disk

If you enable logging to disk for FG-60D and FWF-60D models, Fortinet recommends that you format the log disk using the following CLI command:

```
execute formatlogdisk
Log disk is /dev/sda1.
Formatting this storage will erase all data on it, including logs,
     quarantine files; WanOpt caches; and require the unit to reboot.
Do you want to continue? (y/n) [Enter y to continue]
```

WAN Optimization

In FortiOS 5.0, WAN Optimization is enabled in security policies and WAN Optimization rules are no longer required. Instead of adding a security policy that accepts traffic to be optimized and then creating WAN Optimization rules to apply WAN Optimization, in FortiOS v5.0 you create security policies that accept traffic to be optimized and enable WAN Optimization in those policies. WAN Optimization is applied by WAN Optimization profiles which are created separately and added to WAN Optimization security policies.

MAC address filter list

The `mac-filter` CLI command under the `config wireless-controller vap` setting is not retained after upgrading to FortiOS v5.0 Patch Release 5. It is migrated into both `config user device` and `config user device-access-list setting`.

Spam filter profile

The spam filter profile has been changed in FortiOS v5.0 Patch Release 5. The `spam-emaddr-table` and `spam-ipbwl-table` have been merged into the `spam-bwl-table`. The `spam-bwl-table` exists in the spam filter profile.

Spam filter black/white list

The `config spamfilter emailbwl` and `config spamfilter ipbwl` commands are combined into `config spamfilter bwl`.

DLP rule settings

The `config dlp rule` command is removed in FortiOS v5.0 Patch Release 5. The DLP rule settings have been moved inside the DLP sensor.

Limiting access for unauthenticated users

When configuring User Identity policies, if you select the option *Skip this policy for unauthenticated user* the policy will only apply to users who have already authenticated with the FortiGate unit. This feature is intended for networks with two kinds of users:

- Single sign-on users who have authenticated when their devices connected to their network
- Other users who do not authenticate with the network so are “unauthenticated”

Sessions from authenticated users can match this policy and sessions from unauthenticated users will skip this policy and potentially be matched with policies further down the policy list. Typically, you would arrange a policy with *Skip this policy for unauthenticated user* at the top of a policy list.

You can also use the following CLI command to enable skipping policies for unauthenticated users:

```
config firewall policy
  edit <id>
    set identity-based enable
    set fall-through-unauthenticated enable
    next
  end
```

Use case - allowing limited access for unauthenticated users

Consider an office with open use PCs in common areas. Staff and customers do not have to log in to these PCs and can use them for limited access to the Internet. From their desks, employees of this office log into PCs which are logged into the office network. The FortiGate unit on the office network uses single sign-on to get user credentials from the network authentication server.

The open use PCs have limited access to the Internet. Employee PCs can access internal resources and have unlimited access to the Internet.

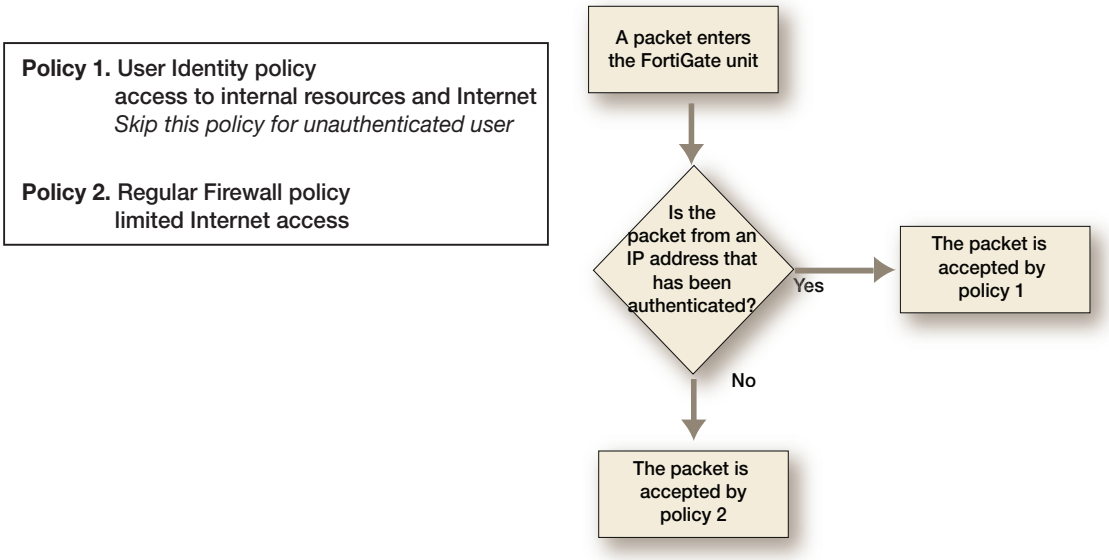
To support these different levels of access you can add a user identity policy to the top of the policy list that allows authenticated users to access internal resources and to have unlimited access to the Internet. In this policy, select *Skip this policy for unauthenticated user*.

Add a normal firewall policy below this policy that allows limited access to the Internet.

Sessions from authenticated PCs will be accepted by the User Identity policy. Sessions from unauthenticated PCs will skip the User Identity policy and be accepted by the normal firewall policy.

Figure 1 shows how the FortiGate unit handles packets received from authenticated and unauthenticated users.

Figure 1: Packet flow for authenticated and unauthenticated users



Use case - multiple levels of authentication

As a variation of the above use case, Policy 2 could be a User Identity policy and *Skip this policy for unauthenticated user* would not be selected. Sessions from unauthenticated users that are accepted by Policy2 would now require users to authenticate before traffic can connect through the FortiGate unit. The result is different levels of authentication: Single sign on for some users and firewall authentication for others.

FortiGate 100D upgrade and downgrade limitations

The following limitations affect the FortiGate 100D model when upgrading from FortiOS v4.0 MR3 to FortiOS v5.0.0 or later.

32-bit to 64-bit version of FortiOS

With the release of FortiOS v5.0.0 or later, the FortiGate 100D will run a 64-bit version of FortiOS. This has introduced certain limitations on upgrading firmware in a high availability (HA) environment and downgrading.

When performing an upgrade from a 32-bit FortiOS version to a 64-bit FortiOS version and the FortiGate 100Ds are running in a HA environment with the uninterruptable-upgrade option enabled, the upgrade process may fail on the primary device after the subordinate devices have been successfully upgraded. To work around this situation, users may disable the uninterruptable-upgrade option to allow all HA members to be successfully upgraded. Without the uninterruptable-upgrade feature enabled, several minutes of service unavailability are to be expected.

Downgrading a FortiGate 100D from FortiOS v5.0.0 or later is not supported due to technical limitations between 64-bit and 32-bit versions of FortiOS. The only procedure to downgrade firmware is by using the TFTP server and BIOS menu to perform the downgrade. In this case the configuration will need to be restored from a previously backed up version.

Internal interface name/type change

In FortiOS v5.0.0 or later the internal interface has been renamed `lan` and the type of the interface has changed to `hard-switch`. In order to create an HA cluster between a FortiGate 100D shipped with FortiOS v5.0.0 or later with a FortiGate 100D upgraded from FortiOS v4.0 MR3, you must first remove the `lan` interface and re-generate the `internal` interface to match the interface on the upgraded device.

Use the following CLI commands to remove the `lan` interface and re-generate the `internal` interface.

```
# config firewall policy
(policy) # purge
  This operation will clear all table!
  Do you want to continue? (y/n)y
(policy) # end

# config system dhcp server
(server) # purge
  This operation will clear all table!
  Do you want to continue? (y/n)y
(server) # end

# config system virtual-switch
(virtual-switch) # purge
  This operation will clear all table!
  Do you want to continue? (y/n)y
(virtual-switch) # end

# config system global
(global) # set internal-switch-mode switch
(global) # end
  Changing switch mode will reboot the system!
  Do you want to continue? (y/n)y
```

Upgrade Information

Upgrading from FortiOS v5.0 Patch Release 3 or later

FortiOS v5.0 Patch Release 5 build 0252 officially supports upgrading from FortiOS v5.0 Patch Release 3 or later.

Please review the Special Notices, Product Integration and Support, Known Issues, and Limitations chapters prior to upgrading. For more information on upgrading your FortiOS device, see the *FortiOS 5.0 Handbook* at http://docs.fortinet.com.

Upgrading an HA cluster

When upgrading a high availability cluster to FortiOS v5.0 patch 5, if uninterruptable-upgrade is enabled you must always upgrade to FortiOS v5.0 Patch 4 before upgrading to patch 5. If you skip this step the firmware upgrade will fail.

Zone-related policies may be deleted when upgrading to FortiOS v5.0 Patch Release 4 or 5

Policies that include interfaces that are members of a zone could be deleted when upgrading to FortiOS v5.0 Patch Release 4 or 5. As of patch release 4 you cannot create policies that include interfaces that have been added to zones. The reason for this restriction is that if you have policies for interfaces added to zones and policies for zones it may not be clear which policy to match with traffic that is received by the interface.

To avoid this problem, review your policies before the upgrade and re-configure policies that include interfaces that have been added to zones.

Captive portal

The captive portal configuration has changed in FortiOS v5.0 Patch Release 5 and upon upgrading the previous configuration may be lost or changed. Review the following configuration examples before upgrading.

Endpoint control

The following examples detail an endpoint control configuration to allow all compliant Microsoft Windows and Mac OS X computers network access. All non-compliant computers will be sent to the captive portal.

***Example FortiOS v5.0.0 configuration*:**

```
edit 3
   set srcintf "internal"
   set dstintf "wan1"
   set srcaddr "all"
   set action accept
   set identity-based enable
```

```
    set identity-from device
    set nat enable
      config identity-based-policy
        edit 1
          set schedule "always"
          set dstaddr "all"
          set service "ALL"
          set devices "windows-pc" "mac"
          set endpoint-compliance enable
        next
        edit 2
          set schedule "always"
          set dstaddr "all"
          set service "ALL"
          set devices all
          set action capture
          set devices "windows-pc" "mac"
          set captive-portal forticlient-compliance-enforcement
        next
      end
    next
```

The new `set forticlient-compliance-enforcement-portal enable` and `set forticlient-compliance-devices windows-pc mac` CLI commands have been added to the master policy. Sub-policy 2 has been removed.

***Example FortiOS v5.0 Patch Release 5 configuration*:**

```
  edit 3
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set action accept
    set forticlient-compliance-enforcement-portal enable
    set forticlient-compliance-devices windows-pc mac
    set identity-based enable
    set identity-from device
    set nat enable
      config identity-based-policy
        edit 1
          set schedule "always"
          set dstaddr "abc"
          set service "ALL"
          set devices "windows-pc" "mac"
          set endpoint-compliance enable
        next
      end
    next
```

After the upgrade, you may experience a configuration loss with the removal of sub-policy 2. If this occurs, you have to enter the following CLI commands:

```
set forticlient-compliance-enforcement-portal enable
set forticlient-compliance-devices windows-pc mac
```

Device detection

The following examples detail a device detection configuration to allow Android, Blackberry, and iPhone devices network access. The captive portal is used to optionally learn the device type, or send back a replacement message if device type cannot be determined.

***Example FortiOS v5.0.0 configuration*:**

```
edit 3
   set srcintf "internal"
   set dstintf "wan1"
   set srcaddr "all"
   set action accept
   set identity-based enable
   set identity-from device
   set nat enable
      config identity-based-policy
         edit 1
            set schedule "always"
            set dstaddr "all"
            set service "ALL"
            set devices "android-phone" "blackberry-phone" "ip-phone"
         next
         edit 2
            set schedule "always"
            set dstaddr "all"
            set service "ALL"
            set devices all
            set action capture
            set captive-portal device-detection
         next
      end
   next
```

The new `set device-detection-portal enable` CLI command has been added to the master policy. Sub-policy 2 has been removed.

***Example FortiOS v5.0 Patch Release 5 configuration*:**

```
edit 3
   set srcintf "internal"
   set dstintf "wan1"
   set srcaddr "all"
   set action accept
   set device-detection-portal enable
   set identity-based enable
   set identity-from device
   set nat enable
      config identity-based-policy
         edit 1
            set schedule "always"
            set dstaddr "abc"
            set service "ALL"
            set devices "android-phone" "blackberry-phone" "ip-phone"
         next
      end
   next
```

After the upgrade, you may experience a configuration loss with the removal of sub-policy 2. If this occurs, you have to enter the following CLI command:

```
set device-detection-portal enable
```

Email collection

The following examples detail an email collection configuration which would allow all devices for which an email-address has been collected network access. Any device which has not had an email collected would be directed to the captive portal.

***Example FortiOS v5.0.0 configuration*:**

```
edit 3
   set srcintf "internal"
   set dstintf "wan1"
   set srcaddr "all"
   set action accept
   set identity-based enable
   set identity-from device
```

```
    set nat enable
      config identity-based-policy
        edit 1
          set schedule "always"
          set dstaddr "all"
          set service "ALL"
          set devices email-collection
        next
        edit 2
          set schedule "always"
          set dstaddr "all"
          set service "ALL"
          set devices all
          set action capture
          set captive-portal email-collection
        next
      end
    next
```

The new `set email-collection-portal enable` CLI command has been added to the master policy. Sub-policy 2 has been removed.

***Example FortiOS v5.0 Patch Release 5 configuration*:**

```
  edit 3
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set action accept
    set email-collection-portal enable
    set identity-based enable
    set identity-from device
    set nat enable
      config identity-based-policy
        edit 1
          set schedule "always"
          set dstaddr "abc"
          set service "ALL"
          set devices "collected-emails"
        next
      end
    next
```

After the upgrade, you may experience a configuration loss with the removal of sub-policy 2. If this occurs, you have to enter the following CLI command:

```
  set email-collection-portal enable
```

Reports

Before you run a report after upgrading to v5.0 Patch Release 5, you must enter the following CLI commands:

```
execute report-config reset
This will reset report templates to the factory default.
All changes to the default report will be lost!
Do you want to continue? (y/n)y
Report configuration was reset to the factory default.


execute report recreate-db
This will recreate the report database from the log database.
Do you want to continue? (y/n)y
Request to recreate report database is successfully sent.
```

SSL VPN web portal

For FG-60C variants and lower models only one SSL VPN web portal is retained after upgrading to FortiOS v5.0 Patch Release 5.

Virtual switch and the FortiGate-100D

The name *Virtual Switch* is used by different objects on the Web-based Manager and the CLI. On the Web-based Manager *Virtual Switch* refers to an interface type and is used for the FortiSwitch controller feature. This instance of *Virtual Switch* maps to the CLI command `config switch-controller vlan`.

The second instance of *Virtual Switch* in the CLI, `config system virtual-switch` is used to configure the hardware switch. This command maps to the Web-based Manager hardware switch interface type.

DHCP sever reserved IP/MAC address list

Up to FortiOS v5.0 Patch Release 4 you could use the following command to add a system-wide reserved IP/MAC address list for all DHCP servers.

```
config system dhcp reserved-address
```

This command has been removed in FortiOS 5.0 Patch Release 5. If you have configured reserved IP/MAC addresses using this command, they will be lost when you upgrade to FortiOS 5.0 Patch Release 5. To keep these IP/MAC address pairs you must add them to individual DHCP server configurations, for example:

```
config system dhcp server
  edit 1
    config reserved-address
      edit 0
        config ip 172.20.120.137
        config mac 00:09:0F:E7:61:40
      end
```

Upgrading from FortiOS v4.0 MR3

FortiOS v5.0 Patch Release 5 build 0252 officially supports upgrade from FortiOS v4.0 MR3 Patch Release 14 and v4.0 MR3 Patch Release 15.

Please review the Special Notices, Product Integration and Support, Known Issues, and Limitations chapters prior to upgrading. For more information on upgrading your FortiOS device, see the *FortiOS 5.0 Handbook* at http://docs.fortinet.com.

Table size limits

FortiOS v5.0 Patch Release 5 has changed the maximum allowable limits on some objects. As a result, the configuration for some objects may be lost. These include:

- `dlp sensor`
- `firewall vip`
- `application list`
- `dlp sensor filter`
- `ips sensor`

For more information, see the *Maximum Values Table for FortiOS 5.0* at http://docs.fortinet.com.

SQL logging upgrade limitation

For the following units, after upgrading to FortiOS v5.0 Patch Release 5 SQL logging will be retained based on the total size of the RAM available on the device. Logs will use up to a maximum of 10% of the RAM. Once passed that threshold, any new logs will overwrite older logs. The historical report generation will also be affected based on the SQL logs that are available for query.

- FG-100D
- FG-300C

SSL deep-scan

A new SSL/SSH inspection option has been added to include all SSL protocols. The protocol status in SSL/SSH inspection will default to *disable* for the SSL protocols. The SSL/SSH inspection should be modified to enable the SSL protocols wherever inspection is required.

Before upgrade

- The antivirus, web filter, and antispam profiles had separate protocol settings for the SSL and non-SSL protocols.
- For HTTPS deep-scanning to be done, deep-scan needed to be enabled for HTTPS in the UTM proxy options.

After upgrade

- The settings for the SSL protocols in the antivirus, web filter, and antispam profiles have been removed. Instead, the non-SSL options will apply to both the SSL and non-SSL versions of each protocol. The SSL/SSH inspection options now includes an enable/disable

option for each protocol. This is used to control which protocols are scanned and which SSL enabled protocols are decrypted.

- To use HTTPS non-deep (SSL handshake) inspection, HTTPS needs to be enabled in the SSL/SSH inspection options. A web filter profile with `https-url-scan` enabled needs to be applied in the policy with the SSL/SSH inspection options. The web filter profile option changes the inspection mode to non-deep scan. AV will not be performed if this option is enabled. The web filter profile option does not apply if SSL inspect-all is enabled in the SSL/SSH inspection options.

Behavior

- After upgrade, all the SSL related settings in the antivirus, web filter, and antispam profiles will be lost. The non-SSL settings will be retained and applied to the related SSL protocols if they are enabled in the SSL/SSH inspection options. The protocol status in the SSL/SSH inspection options will default to enable for the non-SSL protocols and will default to disable for the SSL protocols. The SSL/SSH inspection options should be modified to enable the SSL protocols wherever inspection is required.
- Any profiles requiring non-deep HTTPS inspection will need to be modified to include a web filter profile and SSL/SSH inspection options with the settings as described above. The original HTTPS deep-scan settings will be lost upon upgrade.

Profile protocol options

Deep inspection status configurations are not retained for FTPS/IMAPS/POP3S/SMTPS after upgrading from FortiOS v4.3 MR3.

Example FortiOS v4.3 MR3 configuration:

```
config firewall profile-protocol-options
  edit "default"
    set comment "all default services"
      config http
        set port 80
        set port 8080
        set options no-content-summary
        unset post-lang
      end
      config https
        set port 443
        set port 8443
        set options allow-invalid-server-cert
        unset post-lang
        set deep-scan enable
      end
      config ftp
        set port 21
        set options no-content-summary splice
      end
      config ftps
        set port 990
        set options no-content-summary splice
        unset post-lang
      end
```

```
        config imap
          set port 143
          set options fragmail no-content-summary
        end
        config imaps
          set port 993
          set options fragmail no-content-summary
        end
        config pop3
          set port 110
          set options fragmail no-content-summary
        end
        config pop3s
          set port 995
          set options fragmail no-content-summary
        end
        config smtp
          set port 25
          set options fragmail no-content-summary splice
        end
        config smtps
          set port 465
          set options fragmail no-content-summary splice
        end
        config nntp
          set port 119
          set options no-content-summary splice
        end
      next
    end
```

Example FortiOS v5.0 Patch Release 5 configuration:

```
  config firewall profile-protocol-options
    edit "default"
      set comment "all default services"
        config http
          set ports 80 8080
          set options no-content-summary
          unset post-lang
        end
        config ftp
          set ports 21
          set options no-content-summary splice
        end
        config imap
          set ports 143
          set options fragmail no-content-summary
        end
        config mapi
```

```
            set ports 135
            set options fragmail no-content-summary
          end
          config pop3
            set ports 110
            set options fragmail no-content-summary
          end
          config smtp
            set ports 25
            set options fragmail no-content-summary splice
          end
          config nntp
            set ports 119
            set options no-content-summary splice
          end
          config dns
            set ports 53
          end
        next
      end

    config firewall deep-inspection-options
      edit "default"
        set comment "all default services"
          config https
            set ports 443 8443
            set allow-invalid-server-cert enable
          end
          config ftps
            set ports 990
            set status disable
          end
          config imaps
            set ports 993
            set status disable
          end
          config pop3s
            set ports 995
            set status disable
          end
          config smtps
            set ports 465
            set status disable
          end
        next
      end
```

Upgrade procedure

Plan a maintenance window to complete the firmware upgrade to ensure that the upgrade does not negatively impact your network. Prepare your FortiGate device for upgrade and ensure other Fortinet devices and software are running the appropriate firmware versions as documented in the Product Integration and Support section.

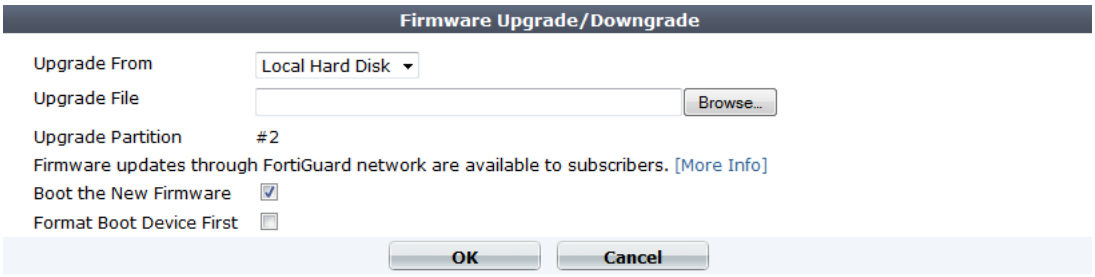
Save a copy of your FortiGate device configuration prior to upgrading. To backup your configuration, go to *System* > *Dashboard* > *Status*. In the *System Information* widget select *Backup* under *System Configuration*. Save the configuration file to your management computer.

To upgrade the firmware via the Web-based Manager:

1. Download the `.out` firmware image file from the Customer Service & Support portal FTP directory to your management computer.
2. Log into the Web-based Manager as the `admin` administrative user.
3. Go to *System* > *Dashboard* > *Status*.
4. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

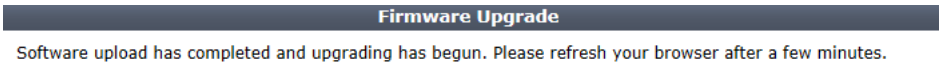
   The *Firmware Upgrade/Downgrade* window opens.

   Figure 2: Firmware upgrade/downgrade window



5. Select *Browse* and locate the firmware image on your management computer and select *Open*.
6. Select *OK*. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version. The following message is displayed.

   Figure 3: Firmware upgrade dialog box



7. Refresh your browser and log back into your FortiGate device. Launch functional modules to confirm that the upgrade was successful.

For more information on upgrading your FortiGate device, see the *Install and System Administration for FortiOS 5.0* at http://docs.fortinet.com/fgt.html.

Downgrading to previous FortiOS versions

Downgrading to previous FortiOS versions results in configuration loss on all models. Only the following settings are retained:

- operation modes
- interface IP/management IP
- route static table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles.

Product Integration and Support

Web browser support

FortiOS v5.0 Patch Release 5 supports the following web browsers:

- Microsoft Internet Explorer versions 9 and 10
- Mozilla Firefox versions 24
- Google Chrome version 28
- Apple Safari versions 5.1 and 6.0

Other web browsers may function correctly, but are not supported by Fortinet.

FortiManager support

FortiOS v5.0 Patch Release 5 is supported by FortiManager v5.0 Patch Release 5.

FortiAnalyzer support

FortiOS v5.0 Patch Release 5 is supported by FortiAnalyzer v5.0 Patch Release 5.

FortiClient support (Windows, Mac OS X, iOS and Android)

FortiOS v5.0 Patch Release 5 is supported by the following FortiClient software versions:

- FortiClient (Windows) v5.0 Patch Release 6 or later
  - Microsoft Windows 8.1 (32-bit and 64-bit)
  - Microsoft Windows 8 (32-bit and 64-bit)
  - Microsoft Windows 7 (32-bit and 64-bit)
  - Microsoft Windows Vista (32-bit and 64-bit)
  - Microsoft Windows XP (32-bit)
- FortiClient (Mac OS X) v5.0 Patch Release 6 or later
  - Mac OS X v10.9 Mavericks
  - Mac OS X v10.8 Mountain Lion
  - Mac OS X v10.7 Lion
  - Mac OS X v10.6 Snow Leopard

See the *FortiClient v5.0 Patch Release 5 Release Notes* for more information.

- FortiClient (iOS) v5.0 Patch Release 2.
- FortiClient (Android) v5.0 Patch Release 2.

FortiAP support

FortiOS v5.0 Patch Release 5 supports the following FortiAP models:

FAP-11C, FAP-14C, FAP-28C, FAP-112B, FAP-210B, FAP-220A, FAP-220B, FAP-221B, FAP-221C, FAP-222B, FAP-223B, FAP-320B, and FAP-320C.

The FortiAP device must be running FortiAP v5.0 Patch Release 6 build 0060 or later.

The FAP-220A is supported on FortiAP v4.0 MR3 Patch Release 9 build 0228.

FAP-221C and FAP-320C

These models are released on a special branch based off of FAP v5.0 Patch Release 6. The branch point reads 060. The FAP-221C firmware has build number 4049. The FAP-320C firmware has build number 4050.

The FAP-320C and FAP-221C models require a special FortiOS build for wireless controller support (FortiOS v5.0 Patch Release 5, branch point 252, build 4396). Firmware images for this special FortiOS build are available from the following directory in the firmware images page of the Customer Service & Support site:

FortiAP/v5.00/5.0/5.0.6/Wireless_controller/

To access this firmware, find the support.fortnet.com page for downloading firmware images, select FortiAP and click the Download button. Then navigate to the folder support.fortinet.com/FortiAP/v5.00/5.0/5.0.6/Wireless_controller/ and download the firmware image for the FortiGate unit that you will be using to manage your FAP-320C or FAP-221C unit. Install this firmware image on your FortiGate unit before installing and managing your FAP-320C or FAP-221C unit.

FortiSwitch support

FortiOS v5.0 Patch Release 5 supports the following FortiSwitch models:

FS-28C, FS-324B-POE, FS-348B, and FS-448B

The FortiSwitch device must be running FortiSwitchOS v2.0 Patch Release 3 build 0010 or later.

FortiOS v5.0 Patch Release 5 supports the following FortiSwitch 5000 series models:

FS-5003B, FS-5003A

The FortiSwitch 5000 device must be running FortiSwitchOS v5.0 Patch Release 3 build 0010 or later.

FortiController support

FortiOS v5.0 Patch Release 5 supports the following FortiController models:

FCTL-5103B

The FCTL-5103B is supported by the FG-5001B and FG-5001C. The FortiController device must be running FortiSwitch 5000 OS v5.0 Patch Release 3 or later.

Virtualization software support

FortiOS v5.0 Patch Release 5 supports the following virtualization software:

- VMware ESX versions 4.0 and 4.1
- VMware ESXi versions 4.0, 4.1, 5.0, and 5.1
- Citrix XenServer versions 5.6 Service Pack 2 and 6.0 or later
- Open Source Xen versions 3.4.3 and 4.1 or later
- Microsoft Hyper-V Server 2008 R2 and 2012
- KVM - CentOS 6.4 (qemu 0.12.1) or later

See "About FortiGate VMs" on page 58 for more information.

Fortinet Single Sign-On (FSSO) support

FortiOS v5.0 Patch Release 5 is supported by FSSO v4.0 MR3 B0143 for the following operating systems:

- Microsoft Windows Server 2012 Standard Edition
- Microsoft Windows Server 2008 R2 64-bit
- Microsoft Windows Server 2008 (32-bit and 64-bit)
- Microsoft Windows Server 2003 R2 (32-bit and 64-bit)
- Novell eDirectory 8.8

FSSO does not currently support IPv6.

Other server environments may function correctly, but are not supported by Fortinet.

FortiExplorer support (Microsoft Windows, Mac OS X and iOS)

FortiOS v5.0 Patch Release 5 is supported by FortiExplorer v2.3 build 1052 or later. See the *FortiExplorer v2.3 build 1052 Release Notes* for more information.

FortiOS v5.0 Patch Release 5 is supported by FortiExplorer (iOS) v1.0.4 build 0118 or later. See the *FortiExplorer (iOS) v1.0.4 build 0118 Release Notes* for more information.

AV Engine and IPS Engine support

FortiOS v5.0 Patch Release 5 is supported by AV Engine v5.146 and IPS Engine v2.173.

Language support

The following table lists FortiOS language support information.

Table 1: FortiOS language support

Language	Web-based Manager	Documentation
English	✔	✔
French	✔	-
Portuguese (Brazil)	✔	-
Spanish (Spain)	✔	-
Korean	✔	-
Chinese (Simplified)	✔	-
Chinese (Traditional)	✔	-
Japanese	✔	-

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 v5.0 Patch Release 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.

Table 2: Supported modules and FortiGate models

AMC/FMC/FSM/RTM Module	FortiGate Model
Storage Module 500GB HDD Single-Width AMC (ASM-S08)	FG-310B, FG-620B, FG-621B, FG-3016B, FG-3810A, FG-5001A
Storage Module 64GB SSD Fortinet Storage Module (FSM-064)	FG-200B, FG-311B, FG-1240B, FG-3040B, FG-3140B, FG-3951B
Accelerated Interface Module 4xSFP Single-Width AMC (ASM-FB4)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Accelerated Interface Module 2x10-GbE XFP Double-Width AMC (ADM-XB2)	FG-3810A, FG-5001A
Accelerated Interface Module 8xSFP Double-Width AMC (ADM-FB8)	FG-3810A, FG-5001A
Bypass Module 2x1000 Base-SX Single-Width AMC (ASM-FX2)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Bypass Module 4x10/100/1000 Base-T Single-Width AMC (ASM-CX4)	FG-310B, FG-311B, FG-620B, FG-621B, FG-1240B, FG-3016B, FG-3810A, FG-5001A
Security Processing Module 2x10/100/1000 SP2 Single-Width AMC (ASM-CE4)	FG-1240B, FG-3810A, FG-3016B, FG-5001A
Security Processing Module 2x10-GbE XFP SP2 Double-Width AMC (ADM-XE2)	FG-3810A, FG-5001A
Security Processing Module 4x10-GbE SFP+ Double-Width AMC (ADM-XD4)	FG-3810A, FG-5001A
Security Processing Module 8xSFP SP2 Double-Width AMC (ADM-FE8)	FG-3810A
Rear Transition Module 10-GbE backplane fabric (RTM-XD2)	FG-5001A
Security Processing Module (ASM-ET4)	FG-310B, FG-311B
Rear Transition Module 10-GbE backplane fabric (RTM-XB2)	FG-5001A

Table 2: Supported modules and FortiGate models (continued)

Security Processing Module 2x10-GbE SFP+ (FMC-XG2)	FG-3950B, FG-3951B
Accelerated Interface Module 2x10-GbE SFP+ (FMC-XD2)	FG-3950B, FG-3951B
Accelerated Interface Module 20xSFP (FMC-F20)	FG-3950B, FG-3951B
Accelerated Interface Module 20x10/100/1000 (FMC-C20)	FG-3950B, FG-3951B
Security Processing Module (FMC-XH0)	FG-3950B

SSL VPN support

SSL VPN standalone client

FortiOS v5.0 Patch Release 5 supports the SSL VPN tunnel client standalone installer build 2294 for the following operating systems:

- Microsoft Windows 8.1 (32-bit & 64-bit), 8 (32-bit & 64-bit), 7 (32-bit & 64-bit), and XP SP3 in `.exe` and `.msi` formats
- Linux CentOS 5.6 and Ubuntu 12.0.4 in `.tar.gz` format
- Mac OS X v10.9, 10.8 and 10.7 in `.dmg` format
- Virtual Desktop in `.jar` format for Microsoft Windows 7 SP1 (32-bit)

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 3: Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 32-bit SP1	Microsoft Internet Explorer versions 8, 9, and 10 Mozilla Firefox version 24
Microsoft Windows 7 64-bit SP1	Microsoft Internet Explorer versions 8, 9 and 10 Mozilla Firefox version 24
Linux CentOS version 5.6 and Ubuntu version 12.0.4	Mozilla Firefox version 5.6
Mac OS X v10.7 Lion	Apple Safari version 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 4: 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 5: 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	✔	✔
Sophos Security Suite	✔	✔
Trend Micro Titanium Internet Security	✔	✔
ZoneAlarm Security Suite	✔	✔
Symantec Endpoint Protection Small Business Edition 12.0	✔	✔

Explicit web proxy browser support

The following web browsers are supported by FortiOS v5.0 Patch Release 5 for the explicit web proxy feature:

- Microsoft Internet Explorer versions 8, 9, and 10
- Mozilla Firefox version 21
- Apple Safari version 6.0
- Google Chrome version 25

Other web browsers may function correctly, but are not supported by Fortinet.

Resolved Issues

The resolved issues tables listed below do not list every bug that has been corrected with FortiOS v5.0 Patch Release 5 build 0252. For inquires about a particular bug, please contact Customer Service & Support.

AntiVirus

Table 6: Resolved antivirus issues

Bug ID	Description
0217761	Hide MAPI option in flow-based antivirus profiles because flow-based antivirus does not support MAPI.

ELBC

Table 7: Resolved ELBC issues

Bug ID	Description
0208715	Corrected an issue with the way that the FG-5001A creates redundant traffic devices in ELBC mode.

Email filtering

Table 8: Resolved Email filtering issues

Bug ID	Description
0203465	Clean up email filtering engine code.
0211955	Email filter ipbwl receive header check method improvements.
0215965	In splice mode, email filtering now correctly extracts recipient information from multiple email messages sent in one session.

Endpoint Control

Table 9: Resolved endpoint control issues

Bug ID	Description
0205229	Endpoint Control now correctly assigns Endpoint Control profiles to AD groups.

Firewall

Table 10: Resolved firewall issues

Bug ID	Description
0170136	The instant messaging (IM) daemon (imd) crashes when processing IM based SIP traffic, such as Yahoo messenger SIP.
0173140	The instant messaging (IM) daemon (imd) crashes when deleting a VDOM and SIP traffic is running.
0189650	Uncompressed size limit blocking for transparent proxy corrected.
0206225	SSL deep inspection no longer causes a browser error in load balancing scenarios.
0209611	Geographic IP addresses do not work with interface policy DoS profiles.
0211591	Users are not matched to all groups when authenticating with a client certificate.
0213572	The amount of memory used by the proxy worker for client comfort replacement messages has been reduced.
0214035	The `auth-policy-exact-match` global option now works correctly.
0214438	NAT64 policies now support Maximum Segment Size (MSS) limiting to avoid fragmentation when packets are converted from IPv4 to IPv6.
0214997	The `auth-secure-http` option now works correctly for IPv6 firewall authentication.
0215908	The client side of the connection now closes correctly when the server sends TCP RST and SSL inspection is enabled.
0216831	SSL proxy stalls when there is no subject CN in the server certificate.
0216947	Returning traffic is not inspected by IPS when a VoIP profile is also added to a policy.
0217302	RADIUS authentication with wildcard admin now works properly.
0218226 0218370	Improved the efficiency of updating the authentication configuration when there are a large number of user accounts.

Firmware upgrades

Table 11: Resolved firmware upgrade issues

Bug ID	Description
0189691	Removed causes of errors in configuration after upgrade.
0211002	Upgrading FortiOS Carrier from V4.0 MR3 to V5.0 no longer removes all Carrier features.
0217412	You can now successfully upgrade a FWF-60CX-ADSL-A from v4.0MR3 to v5.0.

FCTL-5103B

Table 12: Resolved FCTL-5103B issues

Bug ID	Description
0212269	A FortiGate unit displays incorrect trunk information in FortiController dual mode and A-P mode.
0213792	Trunk port not successfully created when members are in use during creation of the trunk.
0214826	Error message `np_xlp_intf_elbc_dev_bind cannot find the device fctrl1/` is seen when the slave is synchronizing with the master.
0216309	A FortiController trunk did not work until reboot.
0217113	Support the explicit proxy GUI for FortiGate in a FortiController cluster.

FG-200D/FG-240D

Table 13: Resolved FG-200D/FG-240D issues

Bug ID	Description
0198221	FG-200D and FG-240D models now support remote FortiSwitch management.

FG-3240C

Table 14: Resolved FG-3240C issues

Bug ID	Description
0214935	HA LED does not turn on.

FG-30D

Table 15: Resolved FG-30D issues

Bug ID	Description
0217986	Add VLAN support.

FG-90D/FWF-90D

Table 16: Resolved FG-90D/FWF-90D issues

Bug ID	Description
0210151, 0213843, 0214232, 0213679	Fixe POE issues including, enable/disable command, debug command, LED and Web-based Manager support.
0214320	STP and 802.1X authentication are missing on all FG-90D models

FortiOS Carrier

Table 17: Resolved FortiOS Carrier issues

Bug ID	Description
0213701	FortiCarrier units do not receive FortiGuard updates when MMS profile virus scanning is enabled.
0217089	Issues with MM1 and MM7 strict-file options resolved.

FortiToken

Table 18: Resolved FortiToken issues

Bug ID	Description
0213701	Token user allowed to authenticate even when token is locked.

High Availability

Table 19: Resolved high availability issues

Bug ID	Description
0112986	HA no longer looses neighbor information after 497 days.
0213203	Gratuitous ARPs are always sent by the primary unit after a split brain configuration occurs.
0215735	The HA management interface default gateway and IP address are no longer lost on the backup unit after virtual clustering is enabled.
0215936	Updates to the geolocation library are now synchronized to the backup unit.

IPS Engine

Table 20: Resolved IPS engine issues

Bug ID	Description
0200658	Application control IDs now appear in traffic logs if deep inspection is enabled for HTTPS-related application control signatures.
0209735, 0209732, 0190277, 0200967, 0200420, 0200436	Corrected issues with nturbo enabled platforms (FG-3600C, FG-3240C, etc) connected with on switching on/off nturbo, and changing IPS engine counts.
0215894 0217407	NAC quarantine now functions correctly when using AV with flow-based inspection mode.

Table 20: Resolved IPS engine issues (continued)

Bug ID	Description
0216702	IPSA no longer takes a long time to compile IPSA rules when the total rule number is large.
0217819	Resolved a Soc2 dfa IPS engine error that caused high CPU use.

IPsec VPN

Table 21: Resolved IPsec VPN issues

Bug ID	Description
0207808	Traffic can now pass through an IP in IP tunnel created using loopback interface IP address.
0209269	If an IP address (v4 or v6) is configured on a dynamic IPsec interface then when a peer connects, attach this IP address to the dynamically created interface.
0209609	When Xauth is not used, certificate information is now correctly reported in IPSec VPN logs.
0209618	Corrected an issue that caused the IPsec Monitor to truncate user names if certificate subject is greater than 64 characters.
0212713	Improved the IKE negotiation performance for dial up peers.
0212924	IKEv2 rekeying when on a busy FortiGate unit no longer causes the IKE daemon to crash.
0213432	IPsec dialup connections are now offloaded to NPx processors after an HA failover.
0213591	IKEv2 work correctly when phase2 proposal authentication is NULL.
0214310	Redundant interfaces now correctly send gratuitous ARP packets if there is a transient link failure.
0215173	HA failover if IPsec packets works correctly for PPPoE interfaces.
0215399	IPsec VPN event log messages are correctly recorded when dead peer detection detects that a peer has failed.
0215961	Windows XP VPN clients can work correctly with NAT Traversal.
0216655	Remote gateway addresses are no longer changed to 0.0.0.0 after rekeying an IKE SA.
0216715	IPsec packets are no longer lost during a rekey sequence with NPx offloading enabled.
0217036	IPsec packets are no longer lost when NPx offload is disabled.
0217704 0145227	Resolved an issue that caused the IKEv2 queue to wait for a pending request that never gets started.

Logging and Reporting

Table 22: Resolved logging and reporting issues

Bug ID	Description
0168040	Broadcast traffic logs are correctly generated in Transparent mode.
0169734	Duplicate log messages are no longer generated for flow-based web filtering when FortiGuard logging and log-all-url options are both enabled.
0194550	Sent and received statistics are now correctly displayed in explicit web proxy utm logs.
0206370	A configuration change event log message will no longer be generated when an administrator logs out without changing the configuration.
0207676	Connection denied messages are correctly generated in Transparent mode when extended traffic logging is enabled.
0210867 0196558 205025 0	The miglogd logging daemon no longer consumes a lot of CPU time when the FortiGate unit is not processing traffic.
0211752	A successful administrator login is now correctly logged as a successful login when the administrator selects decline on the post login banner.
0212410	Event logs and debugs now generated when FortiGate checks for an updated CRL.
0213662	The virus ID and attack ID fields have been added to traffic logs when logging IPS UTM events.
0214229	Firmware upgrade event log added.
0214294	Memory DLP archive removed from memory log setting.
0214755	Filter IP by wildcard from CLI now working correctly.
0216207	The ICMP host unreachable messages now include the correct source and destination addresses.
0216335	Logs are now uploaded to FortiAnalyzer before they are scheduled if the log disk begins to run out of space.
0217511	Changed how searching works in the log message viewer, see “Using wildcard characters when filtering log messages” on page 14.
0217965	Extended traffic logging is enabled in a security policy when you add an application control profile and select traffic logging.

Performance

Table 23: Resolved performance issues

Bug ID	Description

201257	Provide a command to dedicate CPU 0 to management functions (including logging and web-based manager functions). Enabling this option can improve systerm performance and management-related performance and resolve issues that might cause system like IPS to crash. Use the following command to dedicate CPU 0 for management-related processes:
	`config system npu`
	`  set dedicated-management-cpu enable`
	`end`

Remote Switch Management

Table 24: Resolved remote switch management issues

Bug ID	Description
0206830	User defined IP and DHCP range not maintained when authorizing a FortiSwitch unit.
0218531	FG-140D is unable to discover FS-28C.

Routing

Table 25: Resolved routing issues

Bug ID	Description
0203293	IPv6 routing changes are now correctly updated when a FortiGate IPsec interface is brought down and then back up.
0208347	OSPFv3 now correctly adjusts cost according aggregate interface bandwidth.
0209766	IGMP leave message now take effect immediately.
0215787	FortiOS now validates IP addresses and netmasks added to router access lists.
0218336	BGP traps are now sent with the correct BGP peerstate integer.
0218458	Corrected an issue that caused incorrect multicast route-limit error messages.

SSL VPN

Table 26: Resolved SSL VPN issues

Bug ID	Description
0186383	Log messages are now generated when the FortiGate unit sends an SMS message for an SSL VPN user logging in with two-factor authentication.
0200880	Corrected FTP permission issues with SSL VPN web mode.

Table 26: Resolved SSL VPN issues (continued)

Bug ID	Description
0205238	The SSL VPN realm login page now redirects to the right page when the max concurrent user limit is reached.
0205275	The SSL VPN MAC address check error message from SSL VPN clients has been corrected.
0209917	Users can now use the SSL VPN portal to connect to multiple terminal servers behind NAT devices.
0210308	The SSL VPN parser now rewrites URLs properly.
0213616	Corrected errors about how the Fortinet bar interacts with SSL VPN.
0215680	Citrix applications can now get through the SSL VPN portal.
0216630	The SSL VPN tunnel widget now works with Internet Explorer 11.
0216694	SSL VPN users can now login when the incoming interface IP is a VIP address.
0217121	The SSL VPN tunnel mode widget no longer always asks users to download the SSL VPN plugin in Internet Explorer 10 when using the Windows 8 Modern UI.
0217408	Improved SSL VPN portal error checking to resolve an issue that prevented a custom web application from displaying correctly when accessed through the SSL VPN web portal.
0217548	Multicast traffic can now be sent through SSL VPN Tunnels.
0221118 0210435	Incorrect warning messages no longer appear when SSL VPN portal applets are started.

System

Table 27: Resolved System issues

Bug ID	Description
0162895	Entering the command `diagnose npu spm cli 0` no longer crashes the newcli process.
0186459	Corrected an issues that caused a `cmf_shm_api.c error` when adding or deleting VDOMs.
0191869	FortiClient software in downloaded from FortiManager only when `fortimanager-fds-override` is enabled.
0195003	Firewall policies are now validated when added to the FortiGate configuration using a script.
0200719 0213425	The `execute tac report` command no longer crashes the urlfilter daemon.

Table 27: Resolved System issues (continued)

Bug ID	Description
0204694	The connection per second (CPS) rate of a FortiGate unit is no longer reduced when MTU is set to 9000.
0204714	Individual ports on switch interfaces can now be added to aggregate and redundant port configurations.
0207836	FortiGate units now operate correctly with Novatel 551L modems.
0209045	The output of the `show full_configuration` command now includes the first 4 lines of the configuration.
0210159	Installing a corrupted IPS engine package will no longer prevent a FortiGate unit from starting up and operating.
0211188	Administrators with global scope can now correctly access all VDOMs.
0212470	Bridge and ARP limits increased.
0212506	ARM-based FortiGate models should now no experience packet loss with the Sprint Franklin Wireless S600C modem.
0213274	Removed the command `config dhcp reserved-address` because this feature is no longer used. This command created a system-wide IP/MAC address list. Instead you add reserved IP/MAC addresses to individual DHCP servers. For more information, see "DHCP sever reserved IP/MAC address list" on page 25.
0213451	Corrected an issue that stopped IPv6 over IPv4 IPsec traffic from passing through an NP2 processor with offloading enabled.
0213687	Solved a problem that sometimes caused FortiGate units to stop during a firmware upgrade.
0213688	The calculation of shared memory used for quarantine processes is now more efficient.
0213746, 0217083, 0217124	Cache build-up no longer leads to high CPU usage caused by the cmdbsvr and httpsd processes.
0213929	Synp-flood sensors on FG-3810A ADM_XE2 interfaces now function correctly.
0214260	FortiCloud is no longer set as the default logging location by the GUI.
0214341	The dhcpdd daemon no longer crashes if a user ID does not have a terminating character.
0214349	The SSLVPN_TUNNEL_ADDR1 object no longer appears in a Transparent mode VDOM after the configuration is restored.
0214360	The forticron process no longer uses excessive CPU cycles.
0214363	Errors associated with setting the `dhcp-relay-ip` have been corrected.
0214392	Corrected an issue that caused the FortiGate unit to incorrectly display the error message: Token does not belong to this device.

Table 27: Resolved System issues (continued)

Bug ID	Description
0214637	The FortiGate configuration will no longer be corrupted when some CRLs are added.
0214982	FortiGate units no longer limit the number of alert email recipients.
0215019	PPPoE options can no longer be set for loopback and IPsec VPN interfaces.
0215036	TCP traffic is no longer blocked with IPsec and synproxy on ports that are accelerated by XLP processors.
0215107	VLANs added to software switch interfaces now work correctly.
0215113	The mode setting of all FortiGate interfaces is now successful maintained after entering `execute factoryreset2`.
0215361	The FG-100D no longer resets DSCP values.
0215486	Corrected an issue that prevented FortiGate units from generating certificate signing requests (CSRs).
0215866	Inter-VDOM links will continue to work if the type is set to Ethernet.
0216072	Corrections made to errors in the Fortinet FortiGate MIB file generated by the FG-30D.
0216114	Disable a hidden IPMI interface on the FortiGate-3600C.
0216250	Only ports 1 to 18 of the FG-140D can be used for remote FortiSwitch management.
0216579	Corrected an issue that prevented traffic from going through an inter_vdom link between Transparent and NAT mode VDOMs.
0216946	Infected files are no longer submitted to FortiSandbox.
0217034	FortiGate units now correctly respond to NTP requests received through a software switch interface.
0217052	Reply direction packets are no longer copied to other switch interfaces in interface switch mode.
0217224	The firewall policy `clone` CLI command now functions properly.
0217226	FG-3950B XH0 IPv6 and DoS sensors no longer cause high kernel CPU usage.
0217235	More debug information is now available for RADIUS authentication. The RADIUS server name in added to the configuration now appears in fnbamd debug output.
0217257	Timezone settings for Moscow have been corrected.
0217843	Certificate subject names are no longer truncated.

Table 27: Resolved System issues (continued)

Bug ID	Description
0218808	FortiGate units no longer remove UDP checksums from outbound packet.
0219776, 0219463	Corrected an issue with NP4 VLAN interface accounting support that caused a kernel crash.

Upgrade

Table 28: Resolved upgrade issues

Bug ID	Description
0189691	Corrected several upgrade errors.
0211002	Corrected an issues that caused all FortiOS Carrier configuration settings to be lost when upgrading FortiOS Carrier from FortiOS v4.0 MR3 to v5.0.
0217412	You can now upgrade a FWF-60C model from FortiOS v4.0 MR3 to v5.0.

WAN Optimization and Explicit Web and FTP Proxy

Table 29: Resolved WAN optimization and explicit proxy issues

Bug ID	Description
0199986	The explicit web proxy now generates IPS and application control traffic log messages when IPS and application control are enabled.
0200058	HTTPS requests that used a web proxy forwarding server now support deep scanning.
0210010	WAN Optimization peer statistics corrected for FTP.
0212549	Corrected an issue that prevented adding identity based policies to web-proxy polices on some FG-80C units.
0215623	The explicit proxy now detects server certificate changes and regenerates the substituted certificate when deep inspection is enabled.
0215915	Explicit proxy HTTPS connections from Google Chrome to Google websites no longer fail intermittently when SSL deep scan is enabled.
0216804	Corrected an issue that caused exempted URLs to be blocked by explicit web proxy policies that include SSL decryption.
0216869	WAN Optimization no longer crashes when processing pipeline requests when IPS or Application control is enabled.
0217273	Corrected an issue that caused WAN Optimization traffic to be blocked after the `config web-proxy global` configuration is changed.
0217941	Corrected issues that caused intermittent browser errors when using web proxy and NTLM FSSO.

Web-based Manager

Table 30: Resolved Web-based Manager issues

Bug ID	Description
0191565	Corrected an issue that requires a system reboot to access the Web-based Manager.
0210850	The Web-based Manager now correctly shows user names when the users are authenticated against identity-based policy using client certificates.
0214777	The httpsd process no longer crashes when importing CLI commands from the Web-based Manager.
0218370	Corrected an issue that caused the pyfcgid process to use 99.9% CPU to display 30K users in the Web-based Manager.
0221795	FortiGuard DDNS options can now be configured from the Web-based Manager when the interface that you are adding the DDNS options to has been added to a zone.
0221876	The FortiGate SSL VPN portal can now be displayed by Microsoft Internet Explorer 8 and 9 running in compatibility mode.
Multiple	0183458, 0188243, 0214763, 0214576, 0213856, 0187383, 0198597, 0180457, 0204015, 0212203, 0214754, 0206585, 0214259, 0202090, 0213581, 0215028, 0212265, 0186084, 0213636, 0170604, 0214286, 0214644, 0214643, 0201184, 0199724, 0208178, 0200870, 0215442, 0200642, 0216635, 0199879, 0212564, 0204952, 0201314, 0192407, 0174557, 0173239, 0200675, 0200377, 0200794, 0212439, 0200659, 0195223, 0201496, 0192639, 0198469, 0214555, 0212277, 0204268, 0198464, 0178315, 0207869, 0207212, 0215074, 0211354, 0216088, 0213364, 0204094, 0215384, 0175582, 0216213, 0215808, 0216585, 0215480, 0213755, 0216987, 0218403, 0186978, 0217847, 0215031, 0218044, 0218359, 0197140, 0218003, 0214929, 0172119, 0214589, 0214834, 0215321, 0174005, 0218731, 0217483, 0216995, 0217726, 0211199, 0201928, 0217765, 0218057, 0218058, 0201450, 0183671, 0214818, 0206635, 0207781, 0218934, 0218371, 0218370, 0210034, 0214168, 0192187, 0216279, 0216987, 0216576, 0214469, 0219190, 0219579, 0214998, 0206904, 0207402, 0212438, 0213859, 0216544, 0186602, 0206383, 0187925, 0209664, 0195086, 0214816, 0219349, 0220381, 0209062, 0204024, 0221000, 0204024, 0214892, 0194045, 0187716, 0213181, 0214842, 0215780 - Bug fixes.

Web filtering

Table 31: Resolved web filtering issues

Bug ID	Description
0182863, 0211598	The Web Filter process no longer gets stuck in the state: no correct FortiGuard information.

Table 31: Resolved web filtering issues (continued)

Bug ID	Description
0217886	Corrected an issue that caused 99% CPU usage when log-search is enabled in a Web Filter profile.
0219599, 0218486, 0219918, 0220191	Web Filter caching-related fixes.

Wireless

Table 32: Resolved wireless issues

Bug ID	Description
0199911	Scanning event changes are now reflected in the AP-scan log.
0204951	The plus channel is now checked correctly when channel-bonding and DARRP are enabled on the 5GHz band.
0208742	Local-radio now works correctly with custom AP profiles when VDOMs are enabled.
0211456	Captive portal authentication time out now works correctly.
0211772	The default WiFi rekey value (`gtk-rekey-intv`) has been changed from 600 to 3600.
0214470	Corrected a wireless issue that caused DirecTV video on an iPad to stop during DHCP renewal after GTK rekey.
0214725	Corrected an issue that prevented roaming with PMK caching.
0215265	The authentication timeout can now be set correctly in identity-based policies for wireless clients.
0215265	Web-based Manager authentication time out now works correctly.
0216357	Wireless mesh interface address can now be edited/disabled/deleted.
0217552	Corrected a wireless issue that caused throughput to drop off dramatically at distances over 700m even with a strong wireless signal.
0219239	Wireless channel 52 is no longer available on Taiwanese FortiWiFi and FortiAP models.

Known Issues

The known issues tables listed below do not list every bug that has been reported with FortiOS v5.0 Patch Release 5 build 0252. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

FG-1500D and FG-3700D

Table 33: Known FG-1500D and FG-3700D issues

Bug ID	Description
0218425	NP6 syn-proxy does not work.
0210890	IPv6 traffic over IP tunnel cannot pass through if offload is enabled. Workaround: disable offload in tunnel configuration.
0225640	The IPS Engine crashed when viewing top widgets during stress test.
0216235	Fragmented traffic fails to pass IPsec tunnel (4over6/6over6) with default MTU 1500. Workaround: Disable NPU offload in IPsec phase1 setting.
0223686	Traffic history widget cannot report accurate traffic volume at high traffic load in IPS test.
0216496	Multicast over inter-vdom-link does not offload to NP6.

FortiSwitch

Table 34: Known FortiSwitch issues

Bug ID	Description
0220692	Traffic may be interrupted if you have created two physical links between a managed FortiSwitch and a FortiGate acting as the manager but only configured one of the links as an aggregate link member. Workaround: Remove one of the links or configure both of them.

Upgrade

Table 35: Known upgrade issues

Bug ID	Description
0221412	Cannot upgrade a FG-60D HA cluster from build0228 to FortiOS v5.0 Patch Release 5. Workaround: remove the internal and dmz interfaces from the heartbeat devices list before upgrading.
0221684	Dynamic Profile configurations not converted to RSSO when upgrading from FortiOS v4.0 MR3 to v5.0. Workaround: Dynamic Profile configurations must be upgraded manually after upgrading the firmware.

WAN Optimization and explicit proxy

Table 36: Known WAN Optimization and explicit proxy issues

Bug ID	Description
0195564	Application control does not always work as expected for HTTPS traffic over the explicit web proxy.
0222400	WAN Optimization storage not available after a fresh install of FortiOS 5.0 Patch Release 5 on FG-60C and FWF-60C-ADSL models. Workaround: Instead of doing fresh install, upgrade from FortiOS 5.0 Patch Release 4 to Patch Release 5.

Web-based Manager

Table 37: Known Web-based Manager issues

Bug ID	Description

0220056	The Web-based Manager will not display an application sensor properly when the sensor contains an application that is not found in either the built-in or custom application database. This can happen if you enter an application number that does not exist in the database using the following command:
	`config application list`
	`  edit "test-app"`
	`  config entries`
	`  edit 1`
	`  set application 33317`
	`  next`
	`  edit 2`
	`  set application 88888`
	`  next`
	`  end`
	Workaround: Remove the application that has the invalid application number from the CLI.

0220652 0217222	The Web-based Manager may incorrectly display a permission error when entering an incorrect password.

Web Filtering

Table 38: Known Web FIltering issues

Bug ID	Description

0219352	Bing video SafeSearch not working as expected.
	Workaround: You can manually change the URL filter for the Bing search engine to `asyncv2` using the following CLI command:
	`config webfilter search-engine`
	`  edit "bing"`
	`  set url`
	`  "^(\\/images|\\/videos)?(\\/search|\\/async|\\/asyncv2)\\?"`
	`  next`
	You cannot copy and paste this URL into the CLI using a console, SSH or Telnet session because the CLI interprets `?` characters as requesting help. You can type the URL setting in manually, pressing Ctrl+V before entering each ?. From the Web-based Manager you can also enter this command by going to *Config* > *System* > *Advanced* and use the *Upload Bulk CLI Command File* option to upload the command from a text file.

Wireless

Table 39: Known Wireless issues

Bug ID	Description
0212959	The FWF-80CM supports 7 local radio SSIDs.

Limitations

This section outlines the limitations in FortiOS v5.0 Patch Release 5.

Add device access list

If the `device-access-list` has the action set as `deny`, you will need to explicitly define a device in order to allow it to work.

For instance,

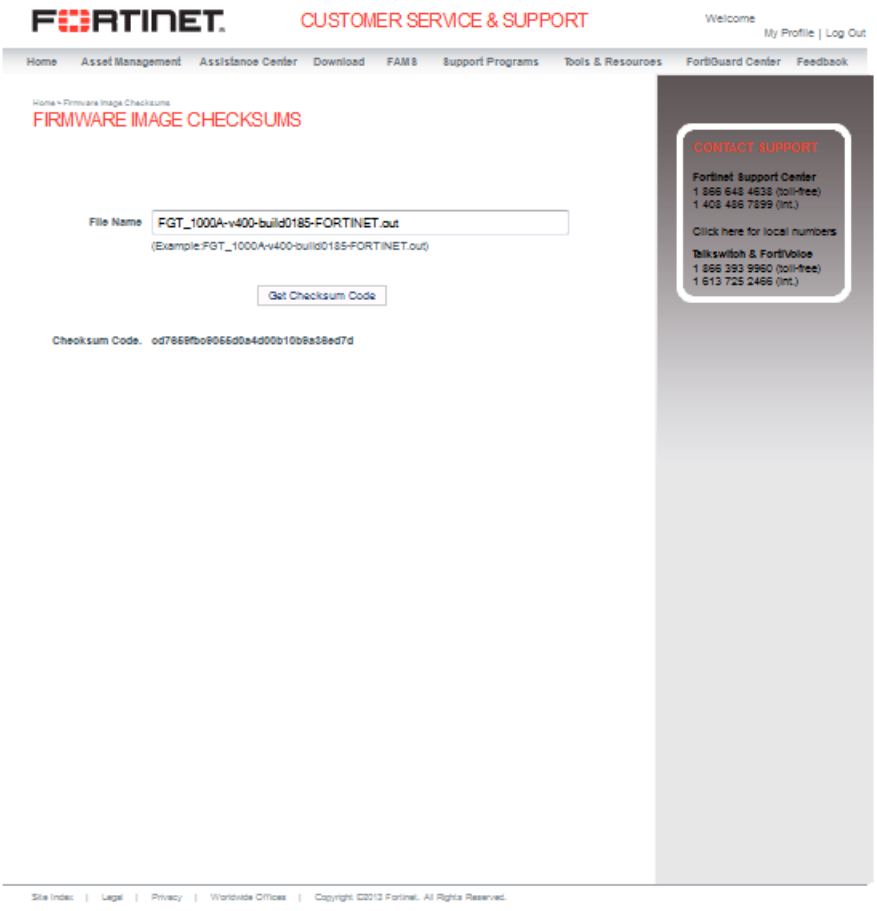
```
config user device
  edit "win"
    set mac 01:02:03:04:05:06
  next
end


config user device-access-list
  edit "wifi"
    set default-action deny
      config device-list
        edit 1
          set action accept
          set device "windows-pc" <-the predefined device-category
        next
        edit 2
          set action accept
          set device "win" <-the custom device
        next
      end
    next
  end
```

As a result, the predefined `device-category` entry 1 will not have network access. Only the custom device entry 2 would be able to get network access.

Firmware Image Checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, select *Download* > *Firmware Image Checksum*, enter the image file name including the extension, and select *Get Checksum Code*.

Figure 4: Firmware image checksum tool



Appendix A: About FortiGate VMs

FortiGate VM model information

Table 40: FortiGate VM model information

Technical Specification	VM-00	VM-01	VM-02	VM-04	VM-08
Virtual CPUs	1	1	1 or 2	1 to 4	1 to 8
Virtual Network Interfaces	2 to 10				
Memory Requirements (GB)	1	2	4	6	12
Storage	30 GB to 2 TB				
VDOMs	1	10	25	50	250
CAPWAP Wireless Access Points	32	32	256	256	1024
Remote Wireless Access Points	32	32	256	256	3072

For more information see the FortiGate VM product datasheet available on the Fortinet web site, http://www.fortinet.com/sites/default/files/productdatasheets/FortiGate-VM01.pdf.

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following VM environments:

VMware

- `.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.

Xen

- `.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 Xen.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix Xen Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

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.

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`.

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 Xen limitations

When using Ubuntu version 11.10, Xen version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.