FortiGate® Multi-Threat Security System

Release Notes

v4.0.0

01-400-84420-20100422

REAL TIME NETWORK PROTECTION

Table of Contents

Change Log

Date	Change Description
2009-02-23	Initial Release.
2009-02-24	Added bug 90024, 91452, 90783, 90499, 90877, and 92102 to Known Issues section. Added FGT-224B to the list of supported models in v4.0.0. Removed checksum for all FOC and FK images. Added checksum for FGT-224B.
2009-02-27	Added D01NE, D02NE, and D11LC modems to supported list. Added [Content Archive Summary] note under section 3.1.
2009-03-09	Added bug 91519 to Known Issues section. Added [RTM Interface Configuration] note under section 3.1.
2009-03-13	Added 'Downgrading to FortiOS v3.00' section.
2009-03-16	Added checksum for FGT-3600.
2009-04-02	Added a note about ASM-SAS module support in the section 1.1. Added section 2.11. Added section 6.11 and 6.12 to list FSAE resolved issues. Added section 2.12.
2009-05-07	Added bug 95098 and 94373 to Known Issues section.
2009-05-26	Updated section 2.1 to include recommended monitor screen resolution and list of supported web browsers. Added Operating System details to section 5.7. Added bug 56258 and 94259 to Known Issues section.
2009-06-05	Added bug 97704 and 93115 to Known Issues section.
2009-06-29	Added Huawei E169 and Sierra Compass 597 to the Supported Modem list.
2009-07-24	Added Huawei E220, Sierra 597E, and Huawei E220 to the Supported Modem list.
2009-12-04	Added modem U300 to the Supported Modem list.
2010-04-22	Fixed a spelling mistake.

Trademarks

Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. 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 guarantees. 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.

Support will be provided to customers who have purchased a valid support contract. All registered customers with valid support contracts may enter their support tickets via the support site:
https://support.fortinet.com

1 FortiOS v4.0.0

This document provides installation instructions, and addresses issues and caveats in FortiOS™ v4.0.0 B0092 release. The following outlines the release status for several models.

Model	FortiOS v4.0.0 Release Status
FGT-30B, FGT-50B, FWF-50B, FGT-60B, FWF-60B, FGT-100A, FGT-110C, FGT-200A, FGT-224B, FGT-300A, FGT-310B, FGT-400A, FGT-500A, FGT-620B, FGT-800, FGT-800F, FGT-1000A, FGT-1000A-FA2, FGT-3016B, FGT-3600, FGT-3600A, FGT-3810A, FGT-5001, FGT-5001A, FGT-5001-FA2, and FGT-5005-FA2.	All models are supported on the regular v4.0.0 branch.

Please visit http://docs.forticare.com/fgt.html for additional documents on FortiOS v4.0.0 release.

1.1 Summary of Enhancements Provided by v4.0.0

The following is a brief list of the new features added in FortiOS v4.0.0.

- Redesigned web UI
- Supports Data Leak Prevention (DLP) Feature
- DHCP over IPSec Interface Support
- Supports Power Supply Monitoring
- WCCP v2 Support
- SNMPv3 Support
- Customized GUI Control
- Enhanced Load Balance Feature
- Supports WAN Optimization and Web Cache Feature
- Redesigned SSL-VPN Web Portal
- Supports HTTP POST Blocking
- Supports Rogue Access Point Detection Feature
- Supports Addition web UI Widgets
- Supports Identity Based Firewall Policies
- Supports Policy Based Traffic Shaping
- Support for IPv6 Intrusion Protection
- Supports "ANY" Interface for Firewall Policies
- Supports ASM-SAS module
- Supports Administration over Modem Interface
- Enhanced Central Management Communication Model
- Redesigned IPS Feature
- RADIUS Feature Enhancements
- Enhanced Application Control Feature
- Configurable VDOM Resource Limits
- Redesigned SNMP MIBS
- Logging Improvements
- Introduction of AntiSpam Engine
- Endpoint Control Feature
- SSL Content Scanning and Inspection
- Administration Over Modem
- Network Access Control (NAC) Quarantine

2 Special Notices

2.1 General

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

IMPORTANT!

Monitor Settings for Web User Interface Access

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

Web Browser Support

- Microsoft Internet Explorer^{TM} 6.0/7.0 and FireFox 2.0x are fully supported.

BEFORE any upgrade

- **[FortiGate Configuration]** Save a copy of your FortiGate unit configuration (including replacement messages) prior to upgrading.

AFTER any upgrade

- **[WebUI Display]** If you are using the Web UI, clear the browser cache prior to login on the FortiGate to ensure proper display of the Web UI screens.
- **[Update the AV/IPS definitions]** The AV/IPS signature included with an image upgrade may be older than ones currently available from the Fortinet's FortiGuard system. Fortinet recommends performing an "Update Now" as soon as possible after upgrading. Consult the FortiGate User Guide for detailed procedures.

2.2 Configuration Files Backups

Configuration files that are backed up in FortiOS v4.0.0 without the encryption option are saved in clear text and are not compressed. It is recommended that you enable encryption for security reasons on the authentication certificates used in VPNs, SSL-VPNs, and administrative access.

2.3 External Modem Support

Configuration of modems on FortiGate models that only support external modems can be performed only through CLI in FortiOS v4.0.0.

2.4 SSL-VPN Notes

The following is a special notice related to the SSL-VPN implementation.

- The "RDP to Host" option web mode can accept a keyboard layout setting as a parameter when the client connects to a server.
    - In the "RDP to Host" field type:
        - <IP address or FQDN of the server> -m <language>
        - <language> is one of the following:
            - ar Arabic

- da Danish
- de German
- en-gb English - Great Britain
- en-us English - US
- es Spanish
- fi Finnish
- fr French
- fr-be Belgian French
- fr-ca French (Canada)
- fr-ch French (Switzerland)
- hr Croatian
- it Italian
- ja Japanese
- lt Lithuanian
- lv Latvian
- mk Macedonian
- no Norwegian
- pl Polish
- pt Portuguese
- pt-br Brazilian Portuguese
- ru Russian
- sl Slovenian
- sv Sedanese
- tk Turkmen
- tr Turkish

2.5 Logging to FortiAnalyzer using AMC Hard Disk

If logging to a FortiAnalyzer is enabled and "Log to AMC Hard Disk & Upload to FortiAnalyzer" option is enabled, all logs are stored on AMC Hard Disk before being sent to FortiAnalyzer. In the event of an AMC hard disk failure, all logs stored on the hard disk waiting to be sent to the FortiAnalyzer may be lost.

2.6 AV Scanning Of Archived Files

The decompression nesting levels for archived files being scanned by the AV engine can now be configured through the CLI. The default decompression level is set to 12.

2.7 WCCP Multi Vdom Support

WCCPv2 is a per-vdom feature, hence the WCCP configuration and webcache should reside on the same vdom. The FortiGate does not support scenarios where WCCPv2 settings are distributed on different vdoms.

2.8 Endpoint Control

Endpoint Control check feature cannot be used with load balance VIP.

2.9 Identity Based Policy

Firewall policy authentication has been reworked in FortiOS v4. Any firewall policy that requires authentication is now known as an Identity Based Policy. You can assign a different schedule, service, protection profile, and traffic shaping to different user groups in one main firewall policy.

2.10 Supported Character Sets

The following lists are the supported character sets by the webfilter and spamfilter features. Please see bug 73616 in the Known Issues section for an important notice related to the supported character sets.

- Japanese
  - jisx0201
  - jisx0208
  - jisx0212
  - sjis
  - euc_jp
  - ISO 2022_jp
  - ISO 2022_jp1
  - ISO 2022_jp2
  - ISO 2022_jp3

- Chinese
  - gb2312
  - euc_cn
  - ces_gbk
  - ces_big5
  - hz
- Korean
  - ksc5601_ex
  - euc_kr
- Thai
  - tis620
  - cp874
- Latin (French, German, Spanish and Italian)
  - ISO 8859_1
  - cp1252
- Serbian, Macedonian, Bulgarian and Russian
  - cp1251

2.11 ASM-SAS Module Support

FortiOS v4 supports ASM-SAS module on the following models:

- FG-5001A-SW
- FG-3810A
- FG-3600A
- FG-3016B
- FG-620B
- FG-310B

2.12 AS Engine Support

AS engine and AS heuristic rule set updates will be supported in a future release for FortiOS.

3 Upgrade Information

3.1 Upgrading from FortiOS v3.00 MR6/MR7

FortiOS v4.0.0 officially supports upgrade from the most recent Patch Release in MR6 or MR7. See the upgrade path below. The arrows indicate "upgrade to".

[MR6]
The upgrade is supported from FortiOS v3.00 B0673 Patch Release 4 or later.

MR6 B0673 Patch Release 4 (or later)
↓
v4.0.0 B0092 GA

After every upgrade, ensure that the build number and branch point match the image that was loaded.

[MR7]
The upgrade is supported from FortiOS v3.00 B0733 Patch Release 2 or later.

MR7 B0733 Patch Release 2 (or later)
↓
v4.0.0 B0092 GA

After every upgrade, ensure that the build number and branch point match the image that was loaded.

[Log Settings Changes]
In FortiOS v4.0.0, the option to configure rule under '`config log trafficfilter`' has been removed, therefore any related configuration is lost upon upgrading from FortiOS MR6 to FortiOS v4.0.0.

[FG-3016B Upgrade]
Interface names on the FGT-3016B have been changed in FortiOS v4.0.0 to match the port names on the face plate. After upgrading from FortiOS MR6 to FortiOS v4.0.0, all port names in the FortiGate configuration are changed as per the following port mapping.

Old port names before upgrading	New port names after upgrading
port1	mgmt1
port2	mgmt2
port3	port1
port4	port2
port5	port3
port6	port4
port7	port5
port8	port6
port9	port7
port10	port8
port11	port9
port12	port10

port13	port11
port14	port12
port15	port13
port16	port14
port17	port15
port18	port16

Note: After the release of FortiOS v3.00 MR6 firmware a new revision of the FGT-3016B included a name change to two ports on the left side of the faceplate. Previously, they were labeled 1 and 2. Now they are called MGMT 1 MGMT 2. However, the BIOS still refers to the MGMT 1 and MGMT 2 ports as port 1 and port 2.

[System Settings]
In FortiOS v4.0.0, the `p2p-rate-limit` setting under `'config system settings'` has been removed, therefore any related configuration is lost upon upgrading from FortiOS MR6/MR7 to FortiOS v4.0.0.

[Router Access-list]
All configuration under `'config router access-list'` may be lost after upgrading from FortiOS v3.0.0 MR6/MR7 to FortiOS v4.0.0.

[Identity Based Policy]
Firewall policy authentication has been reworked in FortiOS v4. Any firewall policy that requires authentication is now known as an Identity Based Policy. Previously, a separate authentication firewall policy had to be created for different schedules, services, and traffic shaping settings but in FortiOS v4 all firewall authentication settings are configured in the Identity Based Policy section of a firewall policy. If no traffic matches any of the Identity Based Policies, the traffic is subjected to an implicit DENY ALL. For example:

In FortiOS v3.00 MR6/MR7

```
config firewall policy
      edit 1
                  set action accept
                  set groups grp1 grp2
                  set service HTTP
                  ...
      next
      edit 2
                  set action accept
                  set service TELNET
            next
            ...
      end
```

After upgrading to FortiOS v4.0.0

```
config firewall policy
      edit 1
                  set action accept
                  set identity-based enable
                        config identity-based-policy
                              edit 1
                                    set groups grp1 grp2
                                    set service HTTP
                                    next
                              end
```

```
            next
            edit 2
                        set action accept
                        set service TELNET
                  next
            end
```

In FortiOS v4.0.0, the TELNET policy is never hit because of the implicit DENY ALL at the bottom of Identity Based Policy. To correct the behaviour, you must move the non-Identity Based Policy (TELNET policy) above the Identity Based Policy.

Reorganized policy in FortiOS v4.0.0

```
      config firewall policy
            edit 2
                  set action accept
                  set service TELNET
                  next
            edit 1
                        set action accept
                        set identity-based enable
                              config identity-based-policy
                                    edit 1
                                          set groups grp1 grp2
                                          set service HTTP
                                    next
                        end
            next
      end
```

[IPv6 Tunnel]
All configuration under `'config system ipv6-tunnel'` may be lost after upgrading from FortiOS v3.0.0 MR7 to FortiOS v4.0.0.

[User Group]
In FortiOS v3.00 a protection profile can be assigned to an user group from web UI, but in FortiOS v4.0 it can only be assigned from CLI.

[Zone Configuration]
In FortiOS v3.00 a Zone name could be upto 32 characters but in v4 it has changed to upto 15 characters. Any Zone names in FortiOS v3.00 with more than 15 characters will be lost after upgrading to FortiOS v4.0.0.

[IPv6 Vlan Interfaces]
Vlan interface with `ipv6-address` configured will be lost after upgrading from FortiOS v3.00 to FortiOS v4.0.0.

[VIP Settings]
`'set http-ip-header'` setting under VIP configuration will inadvertently get set to disable after upgrading from FortiOS v3.00 MR6/MR7 to FortiOS v4.0.0.

[FDS Push-update Settings]
The address and port settings under `'config system autoupdate push-update'` may be lost after upgrading to FortiOS v4.0.0.

[Content Archive Summary]
The content archive summary related configuration will be lost after upgrading to FortiOS v4.0.0.

[RTM Interface Configuration]

Upon upgrading from FortiOS v3.00 MR6/MR7 to v4.0.0, the RTM interface and some of the configuration that uses RTM objects are not retained. In FortiOS v3.00, RTM objects used upper-case letters, such as "RTM/1". FortiOS v4.0.0 uses lower-case letters for RTM objects.

4 Downgrading to FortiOS v3.00

Downgrading to FortiOS v3.00 results in configuration loss on ALL models. Only the following settings are retained:

1. operation modes
2. interface IP/management IP
3. route static table
4. DNS settings
5. VDom parameters/settings
6. admin user account
7. session helpers
8. system access profiles

5 Fortinet Product Integration and Support

5.1 FortiManager Support

FortiOS v4.0.0 is supported by FortiManager v4.0.0.

5.2 FortiAnalyzer Support

FortiOS v4.0.0 is supported by FortiAnalyzer v4.0.0.

5.3 Fortinet Server Authentication Extension (FSAE) Support

FortiOS v4.0.0 is supported by FSAE v3.00 B037 (FSAE collector agent 3.5.037) for the following:

- 32-bit version of Microsoft Windows 2003 Server
- 64-bit version of Microsoft Windows 2003 Server
- 32-bit version of Microsoft Windows 2008 Server
- 64-bit version of Microsoft Windows 2008 Server
- Novell E-directory 8.8.

IPv6 currently is not supported by FSAE.

5.4 AV Engine and IPS Engine Support

FortiOS v4.0.0 is supported by AV Engine 3.00011 and IPS Engine 1.00117.

5.5 3G MODEM Support

The following models and service providers were tested.

Service Provider	3G Card	Identification (IMEI)	Datacard Firmware
Canada			
Telus	ZTE MY39	-	P650M1V1.0.2_Telus_060331
Rogers	Option Globetrotter Qualcomm 3G GX0202	352115011023553	1.10.8Hd
Rogers	Huawei E220	358191017138137	11.110.05.00.00
Rogers	Sierra AirCard 595	-	p1906000,5077
APAC			
E-Mobile	NEC Infrontia Corporation D01NE	-	-
E-Mobile	NEC Infrontia Corporation D02NE	-	-
E-Mobile	Longcheer Holdings Limited D11LC	353780020859740	LQA0012.1.2_M533A
AMER			
Telecom	Sierra Compass 597	-	Rev 1.0 (2), p2314500,4012
Optus	Huawei E169	358109021556466	11.314.17.00.00
Hutchison/3	Huawei E220	358191017339891	11.117.09.00.100
Telecom	Sierra 597E	-	p2102900,4012
Vodafone	Huawei E220	354136020989038	11.117.09.04.00

Service Provider	3G Card	Identification (IMEI)	Datacard Firmware
Soul/TPG	Huawei E220	358193016941644	11.117.08.00.00
Sprint	Franklin Wireless Co. U300	ESN: 0x3B05D354	S/W Ver 68CMU15, H/W Ver 0.3B

5.6 AMC Module Support

FortiOS v4.0.0 supports AMC removable modules. These modules are not hot swappable. The FortiGate must be turned off before the module is inserted or removed.

AMC Modules	FortiGate Support
Internal Hard Drive (ASM-S08)	FGT-310B FGT-620B FGT-3016B FGT-3600A FGT-3810A FGT-5001A-SW
Single Width 4-port 1Gbps Ethernet interface (ASM-FB4)	FGT-310B FGT-620B FGT-3016B FGT-3600A FGT-3810A FGT-5001A-SW
Dual Width 2-port 10Gbps Ethernet interface (ADM-XB2)	FGT-3810A FGT-5001A-DW
Dual Width 8-port 1Gbps Ethernet interface (ADM-FB8)	FGT-3810A FGT-5001A-DW
Single Width 2-port Fiber 1Gbps bypass interface (ASM-FX2)	FGT-310B FGT-620B FGT-3016B FGT-3600A FGT-3810A
Single Width 4-port Ethernet bypass interface (ASM-CX4)	FGT-310B FGT-620B FGT-3016B FGT-3600A FGT-3810A FGT-5001A-SW

5.7 SSL-VPN Support

5.7.1 SSL-VPN Standalone Client

FortiOS v4.0.0 supports the SSL-VPN tunnel client standalone installer B2010 for the following:

- Windows in .exe and .msi format
- Linux in .tar.gz format
- Mac OS X in .dmg format

- Virtual Desktop in .jar format for Windows XP and Vista

The following Operating Systems were tested.

Windows	Linux	Mac OS X
Windows XP 32-bit SP2	CentOS 5.2 (2.6.18-el5)	Leopard 10.5
Windows XP 64-bit SP1	Ubuntu 8.0.4 (2.6.24-23)	
Windows Vista 32-bit SP1		
Windows Vista 64-bit SP1		
Virtual Desktop Support		
Windows XP 32-bit SP2		
Windows Vista 32-bit SP1		

5.7.2 SSL-VPN Web Mode

The following browsers and operating systems were tested with SSL-VPN web mode.

Operating System	Browser
Windows XP 32-bit SP2	IE6, IE7, and FF 3.0
Windows XP 64-bit SP1	IE7 and FF 3.0
Windows Vista 32-bit SP1	IE7, IE8, and FF 3.0
Windows Vista 64-bit SP1	IE7 and FF 3.0
CentOS 5.2 (2.6.18-el5)	FF 1.5 and FF 3.0
Ubuntu 8.0.4 (2.6.24-23)	FF 3.0
Mac OS X Leopard 10.5	Safari 3.2

5.8 SSL-VPN Host Compatibility List

The following Antivirus and Firewall client software packages were tested.

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

6 Resolved Issues in FortiOS v4.0.0

The resolved issues listed below does not list every bug that has been corrected with this release. For inquires about a particular bug, contact Customer Support.

6.1 Command Line Interface (CLI)

Description: "`get router info routing-table`" command is missing from FortiGate's CLI.
Bug ID: 78572
Status: Fixed in v4.0.0.
Affected Models: FGT-30B

Description: Adding a duplicate server entry under directory services may print an error message on FortiGate's console.
Bug ID: 78378
Status: Fixed in v4.0.0.

Description: User group used by a remote administrator user cannot be renamed from CLI.
Bug ID: 76810
Status: Fixed in v4.0.0.

6.2 Web User Interface

Description: Logs for DLP feature cannot be filtered from web UI.
Bug ID: 81652
Status: Fixed in v4.0.0.

6.3 System

Description: FortiGate fails to connect to pppoe server in its first try.
Bug ID: 76864
Status: Fixed in v4.0.0.

Description: Uploading large configuration, using "Upload Bulk Command File" option in web UI, may fail if multiple vdoms are configured.
Bug ID: 78283
Status: Fixed in v4.0.0.

Description: The FortiGate reports an incorrect hard disk capacity through SNMP.
Bug ID: 64544
Status: Fixed in v4.0.0.

Description: Fabric1 and Fabric2 interface status may change to up when show-backplane-intf setting is changed to disable.
Bug ID: 77236
Status: Fixed in v4.0.0.

Description: Modem settings, on FortiGates without internal modem, may be lost after rebooting the unit if modem interface is in non-root vdom.
Bug ID: 78131
Status: Fixed in v4.0.0.

Description: FortiGate does not block oversize icmp6 packets.
Bug ID: 83714
Status: Fixed in v4.0.0.

6.4 High Availability

Description: Slave is unable to Telnet or SSH using master's routing table.
Bug ID: 77989
Status: Fixed in v4.0.0.

Description: Master FortiGate is unable to sync default route to slave after HA mode is changed.
Bug ID: 78461
Status: Fixed in v4.0.0.

Description: The FortiGate incorrectly allows user to configure an interface as pptp-client when HA mode is enabled.
Bug ID: 78489
Status: Fixed in v4.0.0.

Description: Dynamic routing may not work properly on FortiGate unit that has been disconnected from HA cluster using `"exe ha disconnect"` command.
Bug ID: 76687
Status: Fixed in v4.0.0.

Description: Traffic shaping may not work for ftp sessions after a HA failover.
Bug ID: 75261
Status: Fixed in v4.0.0.

Description: "Override disabled" feature does not work when virtual cluster2 is enabled.
Bug ID: 84651
Status: Fixed in v4.0.0.

Description: `"lacp-ha-slave disable"` does not work as expected.
Bug ID: 88935
Status: Fixed in v4.0.0.

6.5 Router

Description: Routes for 192.168.254.X/32 subnet may not be stored in the OSPF LSDB and will not be included in the announcement.
Bug ID: 78450
Status: Fixed in v4.0.0.

Description: IBGP route local-preference and MED may be changed by the inbound route map when FortiGate is configured as route reflector.
Bug ID: 78183
Status: Fixed in v4.0.0.

Description: An interface being used in a static route can be moved to another vdom.
Bug ID: 78461
Status: Fixed in v4.0.0.

6.6 VPN

Description: The SSL-VPN web mode may fail to access websphere applications on APACHE server, an error message `"The Web page cannot be found"` may get displayed.
Bug ID: 77731
Status: Fixed in v4.0.0.

Description: Default setting for "perfect forward secrecy (PFS)" in Phase2 is different when configured from CLI and GUI.
Bug ID: 74822
Status: Fixed in v4.0.0.

Description: The FortiGate fails to provide a DHCP lease to clients over IPSec that are using the same subnet.
Bug ID: 62564
Status: Fixed in v4.0.0.

Description: SSLVPN user cannot login using IE6 browser if content inspection is enabled.
Bug ID: 88287
Status: Not a bug.
Workaround: Disable '`ssl-send-empty-frags`' option.

6.7 WAN Optimization

Description: Wan Optimization does not work for MAPI.
Bug ID: 87405
Status: Fixed in v4.0.0.

6.8 AntiVirus

Description: AV scanning fails on NNTP POST operations.
Bug ID: 50047
Status: Fixed in v4.0.0.

6.9 VOIP

Description: Phone may fail to register when registration request needs to pass through two VDOM's with the SCCP enabled in the Protection profile.
Bug ID: 78297
Status: Fixed in v4.0.0.

6.10 Log & Report

Description: User may not be able to view quarantined files from FortiGate web UI when vdoms are enabled and quarantine is set to FortiAnalyzer.
Bug ID: 77926
Status: Fixed in v4.0.0.

Description: No download link is available for Summary Reports on the Log & Report > Report Access page.
Bug ID: 63740
Status: Fixed in v4.0.0.

6.11 FSAE Collector Agent

Description: A new "Show Service Status" button is added to show detailed status of the service and connected FortiGates.
Bug ID: 84806
Status: Fixed in FSAE collector agent 3.5.037.

Description: A new "Show Monitored DCs" button is added to show the detailed information of connected DC agents.
Bug ID: 84809
Status: Fixed in FSAE collector agent 3.5.037.

Description: A new "Show Logon Users" button is added to show the currently logged on users.
Bug ID: 84808
Status: Fixed in FSAE collector agent 3.5.037.

Description: A new "Log logon events in separated logs" checkbox is added to log user logon related information in a separate log file, and a "View Logon Events" button is added to view these logs.
Bug ID: 84808
Status: Fixed in FSAE collector agent 3.5.037.

Description: The 'AD access mode' drop down list has been moved into a popup window that can be accessed by clicking the button called 'Set Directory Access Information' and the option name has been changed from "NT-style Domain Mode" or "Active Directory Native Mode" to "Standard" or "Advanced".
Bug ID: 84811
Status: Fixed in FSAE collector agent 3.5.037.

6.12 FSAE Windows DC Agent

Description: Two user options are added to the registry. ([HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\dcagent])
1) donot_resolve: If this key value is set to 1, DC Agent will NOT resolve workstation name to IP.
2) no_keepalive: If this key value is set to 1, DC Agent will NOT send keepalive packet to the Collector Agent.
Bug ID: 88707, 84806
Status: Fixed in FSAE collector agent 3.5.037.

7 Known Issues in FortiOS v4.0.0

This section lists the known issues of this release, but is NOT a complete list. For enquiries about a particular bug not listed here, contact Customer Support.

7.1 Command Line Interface (CLI)

Description: `'config antivirus service'` command may show an error when used in vdoms.
Bug ID: 84785
Status: To be fixed in a future release.

Description: FortiGate's console may show "sys_fsae.c:390:[296]" error message when a FSAE server entry under User > Directory Service page is refreshed from web UI.
Bug ID: 87310
Status: To be fixed in a future release.

Description: `'diagnose autoupdate versions'` command does not show correct contract information for AS Rule Set and AS Engine.
Bug ID: 91430
Status: To be fixed in a future release.

Description: Setting max-lines value under `'config log memory global-setting'` close to maximum may cause error messages on console and in some cases may freeze the console.
Bug ID: 91445
Status: To be fixed in a future release.

7.2 Web User Interface

Description: When creating a policy route from web UI, the destination port numbers are not saved if protocol number is set to zero.
Bug ID: 78402
Status: To be fixed in a future release.

Description: The 'Top Viruses' and 'Top Attacks' widget in the System > Status web UI page in Simplified Chinese and Traditional Chinese language using FireFox 2.0 browser may not display the heading properly.
Bug ID: 78344
Status: To be fixed in a future release.

Description: The web UI does not warn the user that an SMTP signature is too long and consequently truncates the signature to 1000 characters.
Bug ID: 65422
Status: To be fixed in a future release.

Description: System > Network > Interface web UI page does not display link status for wlan interface.
Bug ID: 78221
Status: To be fixed in a future release.

Description: The System > Network > Interface web UI page displays incorrect MTU value after override is disabled.
Bug ID: 70688
Status: To be fixed in a future release.

Description: SSLVPN client portal logon page sometimes may not get displayed when using Safari browser on MacOS.
Bug ID: 90509
Status: To be fixed in a future release.
Workaround: Clear the Safari browser cache.

Comment: Safari browser is not officially supported, use IE or FireFox.

Description: Refreshing the Wanopt > Monitor web UI page resets all page filters.
Bug ID: 90479
Status: To be fixed in a future release.

Description: The web UI does not load the IPv6 firewall policy edit page correctly when the FortiGates with special BIOS is running FortiCarrier image.
Bug ID: 91533
Status: To be fixed in a future release.
Models Affected: FortiGate unit with special BIOS running FortiCarrier firmware.

Description: web UI shows an error when an user group is created with the same name as a pki user.
Bug ID: 90499
Status: To be fixed in a future release.

7.3 System

Description: If a FortiGate using ASM-CX4/FX2 module has multiple VDOMs configured and atleast one of the VDOM is in TP mode then user is allowed to enable amc bypass mode even if all ASM-CX4/FX2 interfaces are assigned to NAT VDOM.
Bug ID: 91519
Status: To be fixed in a future release.

Description: The dhcp relay agent does not handle broadcast flag properly.
Bug ID: 93115
Status: Fixed in v4.0.3.

Description: ASM-FB4/FB8 interfaces with fiber SFP may not work when interface speed is set to 1000full.
Bug ID: 90674
Status: To be fixed in a future release.

Description: LDAP user search on active directory does not support range retrieval.
Bug ID: 94259
Status: To be fixed in a future release.

Description: ASM-CX4/FX2 card with firmware 1.0.0 cannot be detected after FortiGate is rebooted.
Bug ID: 90316
Status: To be fixed in a future release.

Description: Traffic going through ASM-FX2 card keeps getting bypassed when ASM-CX4 card is used in slot1 and ASM-FX2 card is used in slot2 and `bypass-mode` is set to disable.
Bug ID: 90017
Status: To be fixed in a future release.

Description: LDAP Distinguished Name query does not work with Windows 2003 or Windows 2008 server.
Bug ID: 68279
Status: To be fixed in a future release.

Description: "Dashboard Statistics" settings in protection profile are selected by default and can cause performance issues when antivirus is not enabled.
Bug ID: 84234
Status: To be fixed in a future release.

Description: "Run image without saving" option may fail when tftp burning an image to FortiGate from BIOS menu.
Bug ID: 91310

Status: To be fixed in a future release.

Description: The count field in an IPv6 firewall policy will incorrectly show the same count value of an IPv4 policy with the same policy id.
Bug ID: 91528
Status: To be fixed in a future release.

Description: WAN-Optimization and Load Balance SSL Offloading does not support 4096-bit certificate.
Bug ID: 91535
Status: To be fixed in a future release.

Description: Traffic Shaping cannot be configured for P2P applications.
Bug ID: 91890
Status: To be fixed in a future release

Description: `snmpd` may spike to 99.9 % CPU usage and snmpwalk may timeout if FortiGate has a big ARP table with more than 300k neighbors.
Bug ID: 90024
Status: To be fixed in a future release.

Description: Maximum numbers of usergroups that can be created is 99 instead of 100.
Bug ID: 91452
Status: To be fixed in a future release.

Description: SNMP polling for HA slave does not work if management vdom is a non-root vdom.
Bug ID: 90783
Status: To be fixed in a future release.

Description: ssl.<vdom> default interface does not get deleted once the vdom is deleted.
Bug ID: 92102
Status: To be fixed in a future release.

Description: `vsd` daemon may randomly crash when under heavey load.
Bug ID: 90877
Status: To be fixed in a future release.

7.4 High Availability

Description: The master unit in an A-A mode cluster stops load-balancing when a redundant link interface on the slave unit is unplugged.
Bug ID: 58959
Status: To be fixed in a future release.

Description: Slave FortiGate's console may show unexpected sync messages while syncing with the master.
Bug ID: 90341
Status: To be fixed in a future release.

Description: The output of some commands, like '`get system status`', are not correct when retrieving information from another member using '`exe ha manage`'.
Bug ID: 56258
Status: To be fixed in a future release.

Description: HA cluster in a-a mode may fail to sync when multiple vdoms are moved from 'virtual cluster 1' to 'virtual cluster 2' and management vdom is changed.

Bug ID: 89681
Status: To be fixed in a future release.

Description: Sessions will not get synced to slave if "Dashboard Statistics" is selected in protection profile. "Dashboard Statistics" are enabled by default.
Bug ID: 87623
Status: To be fixed in a future release.

Description: In an HA cluster a member without AMC module can become master, over a member with an AMC module, if it has a higher priority.
Bug ID: 91001
Status: To be fixed in a future release.

7.5 Router

Description: IPv6 static routes exists in kernel even if gateway is unable to route.
Bug ID: 90473
Status: To be fixed in a future release.

Description: IPv6 static route cannot be added to kernel if route is configured before ipv6 interface address configuration.
Bug ID: 90495
Status: To be fixed in a future release.

7.6 Firewall

Description: Protection profile is not effective when in SSL offload mode.
Bug ID: 97704
Status: To be fixed in a future release.

Description: User is unable to access web pages, hosted on Zope server, when traffic is going through FortiGate's http proxy.
Bug ID: 78246
Status: To be fixed in a future release.

Description: Live streaming radio traffic from www.live365.com does not pass through the FortiGate if http proxy is enabled.
Bug ID: 70963
Status: To be fixed in a future release.

Description: Traffic **c**ount on firewall policy will get reset to zero after an HA failover.
Bug ID: 91028, 83105
Status: To be fixed in a future release.

Description: Protection profile does not get enforced on a firewall policy using virtual server.
Bug ID: 91304
Status: To be fixed in a future release.

Description: Firewall protection profile may not work when in SSL offload mode.
Bug ID: 97704
Status: To be fixed in a future release.

Description: HTTP POST data may be lost if firewall authentication timeout in middle of a session.
Bug ID: 76311
Status: To be fixed in a future release.
Workaround: Enable `auth-keepalive`

7.7 Antivirus

Description: The FortiGate fails to block HTTP POST operations when the protection profile is configured to block banned words.
Bug ID: 61940
Status: To be fixed in a future release.

Description: File pattern list is not effective if the list exceeds 125 entries.
Bug ID: 90096
Status: To be fixed in a future release.

Description: AV scan for NNTP traffic does not work when 'Inspect All Ports' is set for NTTP under Protocol Recognition.
Bug ID: 91585
Status: To be fixed in a future release.

Description: If a server requires client-side certificate and SSL inspection feature is enabled then the connection will be blocked by the FortiGate. SSL Inspection should not play man-in-the-middle for sessions which uses client certificate.
Bug ID: 87297
Status: To be fixed in a future release.

7.8 IPS

Description: Blocking Gmail in application control causes all Google account services to be blocked.
Bug ID: 91403
Status: To be fixed in a future release.

Description: '`DoS Policy`' does not work when two vlans are configured under the same physical interface and are used in two different vdoms.
Bug ID: 91448
Status: To be fixed in a future release.

7.9 Web Filter

Description: The webfilter banned word option does not list Russian as a supported language option for the cyrillic language encoding.
Bug ID: 73616
Status: To be fixed in a future release.

7.10 Data Leak Prevention

Description: There is no valid range of value defined for `quarantine-expiry` setting under ips sensor.
Bug ID: 89091
Status: To be fixed in a future release.

Description: DLP does not block emails encoded with non UTF-8 charset.
Bug ID: 85945
Status: To be fixed in a future release.

Description: DLP rules does not take effect after rebooting the FortiGate.
Bug ID: 91680
Status: To be fixed in a future release.

7.11 Instant Message

The following IMs and their versions were tested in FortiOS v4.0.0. As some IM clients use encrypted connections, the FortiGate may not succeed in blocking the traffic from traversing the firewall.

IM Client	Versions	Comment
AIM	6.8.14.6	This IM version uses SSL communication and FortiGate can only Block or Allow it using firewall policy.
AIM Classic	5.9.6089	none
ICQ	6.5 Build 1005	none
Yahoo! Messenger	9.0.0.2112	none
MSN Live Messenger	8.5.1302.1018	none

Description: The following table lists the known issues with each of the IMs supported by FortiOS v4.0.0.
Models Affected: All
Bug ID: See table

Clients Affected	Versions	Description/Models Affected/Status/BugID
MSN Live Messenger (MSN2009)	14.0.8050	**Description:** IM proxy cannot block or log file transfers for users using MSN Live messenger 14.0.8050. **Status:** To be fixed in a future release. **Bug ID:** 88310

7.12 Peer-to-Peer (P2P)

Description: IPS Engine 1.00092 has made improvements to the blocking functionality of Skype. However, the Skype protocol can be blocked for only a short period.
Bug ID: 37845
Status: To be fixed in a future release.

Description: IM, P2P & VoIP > Statistics > Summary page may not show accurate P2P usage statistics.
Bug ID: 76943
Status: To be fixed in a future release.

Description: P2P blocking and ratelimiting does not work for clients using EMULE (v0.40 or higher) to connect to both the eDonkey network and the Kad network.
Bug ID: 84692
Status: To be fixed in a future release.

7.13 Application Control

Description: An application set to pass may still get blocked if a second 'block all application' rule is added to the same list.
Bug ID: 91669
Status: To be fixed in a future release.

7.14 VPN

Description: SSL host third-party antivirus check plug-in does not detect AVG antivirus scanner.
Bug ID: 89356
Status: To be fixed in a future release.

Description: SSLVPN TELNET and SSH applet only supports ISO/IEC 8859-1 encoding. Characters with other encodings may freeze the applet.

Bug ID: 90642
Status: To be fixed in a future release.

Description: If a SSLVPN firewall policy has both a PKI user and a local user configured, then when a local user authenticates with the FortiGate device it is forced to provide a client certificate and fails to login.
Bug ID: 90428
Status: To be fixed in a future release of the SSL-VPN Client.

Description: When SSLVPN user group host check is enabled, the user using FireFox browser cannot login to SSLVPN.
Bug ID: 95098
Status: To be fixed in a future release.

Description: Renaming an IPSec phase1-interface entry may cause partial loss of firewall policy and network configuration.
Bug ID: 94373
Status: To be fixed in a future release.

7.15 WAN Optimization

Description: FGT-50B-HD does not support iscsi protocol therefore `'config wanopt storage'` command should be removed from the CLI.
Bug ID: 91402
Status: To be fixed in a future release.
Models Affected: FGT-50B-HD

Description: `wad` proxy may crash if 'Cache Explicit Proxy' option is enabled under WAN Opt. > Cache settings.
Bug ID: 91400
Status: To be fixed in a future release.

7.16 Endpoint Control

Description: Endpoints and FortiClient page under `'Endpoint Control'` cannot communicate with FDS if `'Central Management'` option under `'System'` is disabled.
Bug ID: 90625
Status: To be fixed in a future release.

Description: Software Detection cannot detect Bittorrent and Skype programs on the default software detection list.
Bug ID: 90489
Status: To be fixed in a future release.

Description: Endpoint Control does not have its own authentication timeout settings and has to use global `auth-timeout` settings under 'user setting'.
Bug ID: 89552
Status: To be fixed in a future release.

Description: If the difference between the time on the FortiGate and the PC is more than one minute then FortiGate will block all traffic from that PC.
Bug ID: 91471
Status: To be fixed in a future release.

7.17 Log & Report

Description: The FortiGate does not use values for the user and group field in log message for SSL-VPN tunnel activity.
The fields are filled with N/A.
Bug ID: 58836
Status: To be fixed in a future release.

Description: Content archiving of NNTP files is not supported in FortiOS v3.00 MR6 even though the option appears as greyed out implying it may be enabled through another configured option.
Bug ID: 44510
Status: To be fixed in a future release.

Description: Application control logs for IM/P2P are not logged when application entry is configured for "all applications".
Bug ID: 90212
Status: To be fixed in a future release.

Description: A false "Connect to FortiAnalyzer" and "Disconnect from FortiAnalyzer" log is shown when logging to FortiAnalyzer is enabled and a vdom is deleted.
Bug ID: 90686
Status: To be fixed in a future release.

Description: FortiGate incorrectly inserts 5 duplicate log entries when firewall policy with 'Ident based policy' is modified.
Bug ID: 84119
Status: To be fixed in a future release.

Description: IM logs incorrectly shows app_list=N/A.
Bug ID: 89911
Status: To be fixed in a future release.

Description: IPS packet log cannot be viewed from memory and FortiAnalyzer attack logs.
Bug ID: 91450
Status: To be fixed in a future release.

7.18 FSAE (FortiGate)

Description: A redirect warning message is shown on the user's browser after successful FSAE authentication.
Bug ID: 89671
Status: To be fixed in a future release.

8 Image Checksums

```
d13f2eaa379ea49550ade1c5b92a9ec1 *FGT_1000A-v400-build0092-FORTINET.out
862f7926438a99191a3a54f21fcfc47e *FGT_1000AFA2-v400-build0092-FORTINET.out
512d045bbcb3774aaf3f391b41300daf *FGT_1000A_LENC-v400-build0092-FORTINET.out
2239cab588feacd0c223b9e0c2eef7f9 *FGT_100A-v400-build0092-FORTINET.out
34e3d8faf0e215c59709809691085fe0 *FGT_110C-v400-build0092-FORTINET.out
ff478db826d7422b78e92a6aee308d12 *FGT_200A-v400-build0092-FORTINET.out
59479d2b2e4b5d681cdeefcb02971573 *FGT_224B-v400-build0092-FORTINET.out
a7ba74c8e5630afa88b70c670dd46863 *FGT_300A-v400-build0092-FORTINET.out
a41ea75eedf823f82fab3f4c85dc07b1 *FGT_3016B-v400-build0092-FORTINET.out
16217bef0c97e0af9a26480368508fd5 *FGT_30B-v400-build0092-FORTINET.out
0c0ceb0c5eb063bd02c2003cade6856d *FGT_310B-v400-build0092-FORTINET.out
32058183e710ff690dca8c3fe026266e *FGT_3600A-v400-build0092-FORTINET.out
29cf1d0555da4d019310a23715094638 *FGT_3810A-v400-build0092-FORTINET.out
1a83a9acd0687b2e7c7b4063928237c0 *FGT_400A-v400-build0092-FORTINET.out
4a9377561bb30ed6dfbf951a33deaaa7 *FGT_5001-v400-build0092-FORTINET.out
8291ccda3b1e45ce39571772200846cd *FGT_5001A-v400-build0092-FORTINET.out
bcf691ac76890d47acd0c7c27f12a1b9 *FGT_5001FA2-v400-build0092-FORTINET.out
d36607eca8723654b4c6494b1b838800 *FGT_5005FA2-v400-build0092-FORTINET.out
09c63f7597d8a692c4192cc69a02ead3 *FGT_500A-v400-build0092-FORTINET.out
ab4fec24269d470c0441754990fd2e56 *FGT_50B-v400-build0092-FORTINET.out
de35495082fbfc0ce47805e9de2c0c72 *FGT_50B_HD-v400-build0092-FORTINET.out
f34b3228b423dd1036f1aa8f44fab5cd *FGT_60B-v400-build0092-FORTINET.out
98437f018cc91cf8e8f40e15be40cc44 *FGT_620B-v400-build0092-FORTINET.out
72580d16a06f802b1508e46bd8349e4c *FGT_800-v400-build0092-FORTINET.out
b99a8765d585e4bf271b268695736fb2 *FGT_800F-v400-build0092-FORTINET.out
3f705583b179f235f03f0bc5b03305de *FWF_50B-v400-build0092-FORTINET.out
1f4406fd175af43c1ad3d464d6b20056 *FWF_60B-v400-build0092-FORTINET.out
caed4822b9434c7abff53c9bc01b6da0 *FGT_3600-v400-build0092-FORTINET.out
```

9 Appendix A – P2P Clients and Supported Configurations

The following table outlines the supported configurations and related issues with several P2P clients. N/A means either the application does not support the feature or it is not officially tested.

Note: As some P2P clients use encrypted connections, the FortiGate may not succeed in blocking the traffic from traversing the firewall.

	Skype 3.8	**Kazaa 3.2.7**	**BearShare 7.0**	**Shareaza 4.1**	**BitComet 1.0.7**	**eMule 0.49b**	**Azureus 4.0.0.2**	**LimeWire 4.18.8**	**iMesh 8.0**	**DC++ 0707**	**Winny 728**
Standard Ports Direct Internet Connection											
Pass	N/A	N/A	OK	OK	OK	OK	OK	OK	OK	OK	OK
Block	N/A	N/A	OK	OK	OK	OK	OK	OK	OK	OK	OK
Rate Limit	N/A	N/A	Bug ID: 86147	OK	OK	Bug ID: 86452	OK	Bug ID: 77852	OK	N/A	OK
Standard Ports Proxy Internet Connection											
Pass	N/A	N/A	OK	N/A	N/A	OK	OK	OK	N/A	N/A	N/A
Block	N/A	N/A	OK	N/A	N/A	OK	OK	OK	N/A	N/A	N/A
Rate Limit	N/A	N/A	OK	N/A	N/A	Bug ID: 86452	OK	OK	N/A	N/A	N/A
Non-standard Ports Direct Internet Connection											
Pass	OK	OK	N/A	OK	OK	OK	OK	OK	OK	N/A	N/A
Block	Bug ID: 37845	OK	N/A	OK	OK	OK	OK	OK	OK	N/A	N/A
Rate Limit	N/A	OK	N/A	OK	OK	Bug ID: 86452	OK	Bug ID: 77852	OK	N/A	N/A
Non-standard Ports Proxy Internet Connection											
Pass	OK	OK	N/A	N/A	N/A	OK	OK	OK	N/A	N/A	N/A
Block	Bug ID: 37845	OK	N/A	N/A	N/A	OK	OK	OK	N/A	N/A	N/A
Rate Limit	N/A	OK	N/A	N/A	N/A	Bug ID: 86452	OK	Bug ID: 77852	N/A	N/A	N/A

(End of Release Notes.)