



FortiAnalyzer FIPS

Version 4.0

Technical Note

FortiAnalyzer FIPS Technical Note

September 27, 2010

© Copyright 2010 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

| | |
|--|-----------|
| Introduction | 5 |
| Security level summary | 5 |
| FIPs security concerns | 5 |
| Documentation | 6 |
| Fortinet Tools and Documentation CD | 6 |
| Fortinet Knowledge Center | 6 |
| Comments on Fortinet technical documentation | 6 |
| Customer service and technical support..... | 6 |
| Secure operation of FortiAnalyzer units..... | 7 |
| Overview of FIPS compliant operation | 7 |
| Use of non-FIPS compliant features..... | 7 |
| Effects of FIPS compliant mode | 7 |
| Initial configuration of the FortiAnalyzer unit | 8 |
| Installing the unit..... | 8 |
| Registering the unit..... | 8 |
| Downloading and installing FIPS certified firmware..... | 9 |
| Verifying the firmware version of the unit..... | 9 |
| Enabling FIPS mode..... | 10 |
| Configuring interfaces..... | 10 |
| FIPS mode status indicators..... | 10 |
| Administration..... | 10 |
| Administrator roles..... | 11 |
| Administrator accounts and profiles..... | 11 |
| Remote access requirements | 11 |
| Configuration backup..... | 12 |
| Error mode..... | 12 |
| Disabling FIPS mode | 13 |

Introduction

This technical note describes how to install FIPS certified firmware on the FortiAnalyzer unit and how to operate the unit in FIPS compliant mode. It provides information that is not included in the standard documentation provided with your FortiAnalyzer unit.

Federal Information Processing Standards (FIPS) mode is an enhanced security option for some FortiAnalyzer models. Installation of FIPS firmware is required only if the unit was not ordered with this firmware pre-installed.

This document was created as part of the FIPS 140-2 Level 1 validation of the FortiAnalyzer unit and applies only to the models named in the security target document.

This document is intended to be used by a system administrator.

Security level summary

The following FortiAnalyzer units are certified to FIPs140-2 - *Security Requirements for Cryptographic Modules* (FIPS 140-2):

- FortiAnalyzer-100B
- FortiAnalyzer-800
- FortiAnalyzer-800B
- FortiAnalyzer-1000B
- FortiAnalyzer-2000
- FortiAnalyzer-2000A
- FortiAnalyzer-4000
- FortiAnalyzer-4000A

Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website:
<http://csrc.nist.gov/groups/STM/cmvp/index.html>.

FIPs security concerns

The following security issues are not addressed in the standard documentation set.

TSF domain separation

The FortiAnalyzer unit maintains an isolated security domain for its own execution. Specifically:

- No unrelated applications are allowed to run on the FortiAnalyzer unit.
- No unrelated applications can be loaded onto the FortiAnalyzer unit.
- Administrators have no access to the operating system or the file system.
- All security and configuration data are stored in segregated configuration files.

Subset residual data protection

The FortiAnalyzer unit ensures that no residual data from previous packets passing through it is reused in any way. Any residual information in any resource is over-written or otherwise destroyed so that it cannot be reused or otherwise accessed either inadvertently or deliberately.

Restrictive default values

Enabling the FIPS mode of operation changes the configuration of the FortiAnalyzer unit to restrictive default values. For more information, see “Effects of FIPS compliant mode” on page 7. The administrator can override the default values.

Reliable time stamps

The FortiAnalyzer unit provides reliable timestamps using an internal clock that the administrator can set.

Documentation

The documentation for FortiAnalyzer units operated in FIPS mode consists of this technical note and the following documents that comprise the standard FortiAnalyzer™ documentation set for the FortiAnalyzer units:

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Base.

Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of all Fortinet documentation see the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kb.fortinet.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

Secure operation of FortiAnalyzer units

This chapter contains the following sections:

- [Overview of FIPS compliant operation](#)
- [Initial configuration of the FortiAnalyzer unit](#)
- [Administration](#)
- [Error mode](#)
- [Disabling FIPS mode](#)

Overview of FIPS compliant operation

FIPS compliant operation requires both that you use the FortiAnalyzer unit in FIPS mode and that you follow secure procedures for installation and operation of the FortiAnalyzer unit. You must ensure that:

- The FortiAnalyzer unit is installed in a secure physical location.
- Physical access to the FortiAnalyzer unit is restricted to authorized operators.
- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Procedurally, Administrator account passwords must have the following characteristics:
 - One (or more) of the characters should be capitalized.
 - One (or more) of the characters should be numeric.
 - One (or more) of the characters should be non alpha-numeric (e.g. punctuation mark).
- Administration of the FortiAnalyzer unit is permitted using only certified administrative methods. These are:
 - console connection
 - web-based manager via HTTPS
 - command line interface (CLI) access via SSH

Use of non-FIPS compliant features

FIPS mode does not prevent you from using non-FIPS compliant features that are not permanently disabled. If you use these features, however, you are not operating the FortiAnalyzer unit in strict FIPS compliance according to the Security Target.

Effects of FIPS compliant mode

The following list describes, not necessarily in order, the effects of enabling FIPS mode with respect to the normal mode of operation.

Interfaces

- Immediately after switching to FIPS mode, all network interfaces are down and have no IP address assigned. Configure interfaces as needed.
- By default, no network interfaces have administrative access enabled, but all are configured to respond to ping requests.
- Network interfaces cannot be configured for HTTP or Telnet administrative access.

Administration

- Administrative access via HTTPS or SSH requires strong cryptography: AES or 3DES encryption with SHA1 digest. DES encryption and MD5 digest are not available.
- The `get system status` CLI command display includes “FIPS status: enable”.
- Administrators and authenticated users must have passwords at least eight characters long.
- The FortiAnalyzer unit performs self-tests at startup, when initiated by an administrator or when keys are generated. If any of these tests fail, the unit goes into FIPS Error mode and shuts down.
- Remote access clients must meet security requirements. See “[Remote access requirements](#)” on page 11.

Routing

- Immediately after switching to FIPS mode, no DNS addresses are configured.
- Immediately after switching to FIPS mode, no default route is configured.

Logging

- New log messages available for FIPS status reporting (i.e. FIPS error mode)

Initial configuration of the FortiAnalyzer unit

This section describes how to configure your FortiAnalyzer unit in FIPS mode. Proceed as follows:

- Install the unit following the procedures in the documentation.
- Register your FortiAnalyzer unit with Fortinet.
- If you are upgrading an existing FortiAnalyzer unit to FIPS firmware, download the appropriate firmware from Fortinet and install it on your unit.
- Verify the firmware version of your FortiAnalyzer unit.
- Enable FIPS mode.

Installing the unit

Both the **QuickStart Guide** and the **Install Guide** for your FortiAnalyzer unit provide instructions on the physical installation and initial configuration of your unit. When you have completed these procedures you will be able to access both the web-based manager and Command Line Interface (CLI).

Registering the unit

For information about registering your FortiAnalyzer unit, go to the Fortinet Technical Support web site, <https://support.fortinet.com>. You need the user name and password

Fortinet provides to you to download the FIPS certified firmware.

Downloading and installing FIPS certified firmware

Unless you purchased a FortiAnalyzer unit with FIPS firmware pre-installed, you need to download and install the appropriate firmware for your FortiAnalyzer unit. Your FortiAnalyzer unit model must be one of those listed in [“Security level summary” on page 5](#).

Downloading the FIPS/CC certified firmware

The firmware file for each FIPS-validated FortiAnalyzer model is:

Version 4.0.0, build 6087, 091105.

To download the firmware

- 1 With your web browser, go to <https://support.fortinet.com> and log in using the name and password you received when you registered with Fortinet Support.
- 2 Navigate to the version 4.0 FortiAnalyzer Images and Notes page. Select Download Page for the FIPS compliant firmware build. Save the file on the management computer or on your network where it is accessible from the FortiAnalyzer unit.

Installing the FIPS firmware

You can install the FIPS certified firmware as an upgrade from the standard firmware.

To install the FIPS firmware

- 1 Using the management computer, connect to the unit's web-based manager. See the **QuickStart Guide** or the **Install Guide** for information.
- 2 Type admin in the name field. If you have assigned a password, type it in the Password field. Select Login.
- 3 Go to **System > Dashboard > Status**.
- 4 Under System Information > Firmware Version, select Update.
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.

The unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the Login page. This process takes a few minutes.

Verifying the firmware version of the unit

Execute the following command from the command line:

```
get system status
```

The version line of the status display shows the FortiAnalyzer model number, firmware version, build number and date:

```
Version: FortiAnalyzer-800B v4.0,build6087,091105
```

Verify that your firmware version, build number and date match those shown above.

Enabling FIPS mode

If you have verified the firmware version, you are ready to enable FIPS mode. As part of enabling FIPS mode, you must define administrator account names and passwords. The default admin account is not available in FIPS mode. You must use a console connection to enable FIPS mode. If you try to use another type of connection, a “check permission failed” error occurs.



Note: When you enable FIPS mode, all of the existing configuration is lost.

To enable FIPS mode

1 Log in to the CLI using default admin account.

2 Enter the following commands:

```
config system fips
  set status enable
end
```

3 In response to the following prompt, enter the password for the admin account:

```
Please enter administrator name:
```

4 When prompted, re-enter (verify) the admin password.

5 The console displays the following message;

```
Warning: most configuration will be lost,
do you want to continue? (y/n)
```

6 Enter *y*.

The FortiAnalyzer unit will restart in FIPS mode.

Configuring interfaces

When FIPS mode is first enabled, all network interfaces are down and have no IP addresses assigned. This example shows how to configure port1 with an IP address of 192.168.0.99 and administrative access to permit use of the web-based manager.

```
config system interface
  edit port1
    set ip 192.168.0.99 255.255.255.0
    set allowaccess https
    set status up
  end
```

For detailed information about configuring network interfaces, refer to the FortiAnalyzer documentation supplied with your unit.

FIPS mode status indicators

To determine if a FortiAnalyzer is running in FIPS mode, type the following command:

```
get system status
FIPS status: {enabled|disabled}
```

Administration

FIPS mode enforces predefined administrator roles instead of the more granular selection access permissions allowed in the non-FIPS mode of operation.

Administrator roles

In FIPS mode, the module provides two roles for Crypto Officers (hereafter referred to as operators): Crypto Officer and User.

The Crypto Officer role is initially assigned to the default 'admin' operator account.

The Crypto Officer role has read-write access to the module's administrative services. Crypto Officer access to the services can be customized using access profiles. A Crypto Officer with sufficient permissions can create or modify access profiles to limit access to the administrative services. When operator accounts are created, the Crypto Officer specifies an access profile for that operator.

Operators assigned the User role have read-only access to the module's administrative services.

The module does not provide a Maintenance role.

Administrator accounts and profiles

When you invoke FIPS mode for the first time, the FortiAnalyzer unit prompts you for a password for the admin account.

After the initial configuration of administrators when you enable FIPS mode, you can create additional administrator accounts as needed, assigning the appropriate access profile to define each administrator's role. Depending on the administrator roles you initially assigned, one or more of the following preconfigured access profiles are present.

The following table provides a mapping of FortiAnalyzer system roles to FIPS roles:

Table 1: Default administrator access profiles

| FortiAnalyzer System Role | FIPS role |
|---------------------------|----------------|
| admin | Crypto Officer |
| read-only | User |

If necessary, create the access profile that you need. In the web-based manager, when you create the access profile, you select one or more administrator roles. In the CLI, you set the `roles` field to one or more of the following values: `co` for Crypto Officer, `u` for User. For example, to create a profile for the Crypto Officer role, enter

```
config system accprofile
  edit def_prof_CO
    set roles co
  end
```

Remote access requirements

In FIPS mode, remote administration via HTTP or Telnet is disabled as they are not secure. SSH and HTTPS access are permitted but must meet certain security requirements.

Enabling administrative access

In FIPS mode, the network interfaces by default do not allow administrative access, preventing you from using the web-based manager. You can re-enable use of the web-based manager using CLI commands on the console. This example enables HTTPS administrative access on the port1 interface to allow use of the web-based manager and SSH clients:

```
config system interface
  edit port1
    set allowaccess https ssh
```

end

For detailed information about accessing the web-based manager, see “Connecting to the web-based manager” in the *Installation Guide* for your unit.

SSH client requirements

To access the CLI through network interfaces in FIPS mode, your SSH client must support the following:

Authentication:

- RSA X9.31 or HMAC SHA-1

Encryption:

- AES128, AES192, AES256 or 3DES

Web browser requirements

To use the web-based manager in FIPS mode, your web browser application must meet the following requirements:

- Authentication algorithm
 - RSA X9.31, PKCS1 RSA or DSS (in descending order of preference)
- Connection security:
 - TLS 1.0

Configuration backup

Configuration backup files created in FIPS mode are not compatible with backup files created in non-FIPS mode. A FIPS mode configuration backup cannot be restored in non-FIPS mode and vice-versa.

You can create FIPS configuration backup files to use for disaster recovery. They are valid on a replacement FortiAnalyzer unit or to restore configuration after you exit and then re-enter FIPS mode.

For detailed information about creating configuration backup files, refer to the documentation provided with your FortiAnalyzer unit.



Note: Configuration backup or restoration using TFTP is not permitted in FIPS mode.

Error mode

When one or more of the self-tests fail, the FortiAnalyzer unit switches to FIPS Error mode. The FortiAnalyzer unit shuts down all interfaces including the console and blocks traffic.

To resume normal FIPS mode operation, switch the unit off and then on again. If the self-tests pass after the reboot, the unit will resume normal FIPS compliant operation. If a self-test continues to fail after rebooting, there is likely a serious firmware or hardware problem and the unit should be removed from the network until the problem is solved.

If the self-test failure persists across reboots, you can attempt to reload the firmware after resetting the unit to the factory default configuration. If the self-test failure persists after reloading the firmware and re-enabling the FIPS mode of operation, contact Fortinet technical support.

Disabling FIPS mode

The only way that you can return the FortiAnalyzer unit to the normal mode of operation is to restore the factory default configuration. Enter the following CLI command:

```
execute factoryreset
```

Disabling FIPS mode erases the current configuration.

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com