Avaya VPN Client Configuration – FIPS 140-2

Avaya VPN Client
Release 7.11

Document Status: **Standard**

Document Number: **NN46110-510**

Document Version: **02.01**

Date: **November 2010**

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Figures

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- "Getting technical documentation" on page 7
- "Getting product training" on page 7
- "Getting help from a distributor or reseller" on page 8
- "Getting technical support from the Avaya Web site" on page 8

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Preface

This guide provides information about how to configure the Avaya VPN Client to operate in FIPS 140-2 compliant mode.

This guide describes the Avaya VPN Client only in the context of configuring it for FIPS. For more information about Avaya VPN Client software documentation, see *Avaya VPN Router Configuration — Client* Version 7.01 (NN46110-306) 311644-K Rev 02.

Before you begin

This guide is for network managers who are responsible for setting up and configuring the Avaya VPN Client for FIPS 140-2. This guide assumes that you have the following background:

- Experience with system administration
- Familiarity with network management
- Knowledge of FIPS concepts and procedures

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **`ping`** <*`ip_address`*>, you enter **`ping 192.32.10.12`**

`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`show health`** command.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **`show ntp`** `[`**`associations`**`]`, you can enter either **`show ntp`** or **`show ntp associations`**.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`ping`** <*`ip_address`*>, *`ip_address`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `File not found.`
separator (>)	Shows menu paths. Example: Choose Status > Health Check.

Acronyms

This guide uses the following acronyms:

3DES	Triple DES
AES	Advanced Encryption Standard
AH	Authentication Header
DES	Data Encryption Standard
FIPS	Federal Information Processing Standards
HMAC	Hashing Message Authentication Code
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol

IPsec	Internet Protocol Security
KAT	known answer test
MD5	Message Digest 5
NIST	National Institute of Standards and Technology

Related publications

For complete information about installing and configuring the Avaya VPN Client, refer to the following publications (included on the FIPS software CD):

- Avaya VPN Client release notes
- Avaya VPN Router Configuration — Client
- Using Avaya Secure IP Services Gateways In FIPS Mode.

New in this release

The following sections details what is new in *Avaya VPN Client Configuration — FIPS 140-2*. (NN46110-510).

- “Features
- “Other changes

Features

There are no new features in this release.

Other changes

There are no other changes in this release.

Configuring FIPS mode

The Avaya VPN client can run in normal operating mode or in FIPS operating mode. Version 7.11 has FIPS enabled by default. In FIPS operating mode, the Avaya VPN client meets all requirements for FIPS 140-2. (You can find publications for 140-2 and related information at the http://csrc.nist.gov/cryptval/ URL. For the list of Avaya security policies, click on Validation Lists in the left column of the page. For further information, see *Using Avaya Secure IP Services Gateways In FIPS Mode*.

Whenever you are using vendor products such as, for example, MSCAPI and RSA, you must ensure that those products are also FIPS certified. To check for the current information regarding regarding those compliances, see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm.

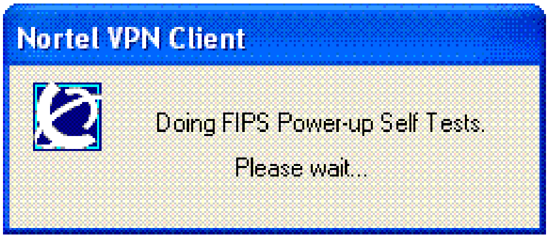
Self tests

To prevent any secure data being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. The client contains self-tests that are run during startup and periodically during operation.

Initialization self tests

When you enable FIPS mode, the client performs startup self-tests (Figure 1).

Figure 1 Power-up self test



Nortel VPN Client

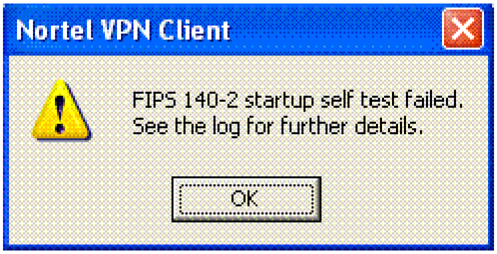
Doing FIPS Power-up Self Tests.

Please wait...

The self tests take approximately 2 seconds on a typical machine (1.8 GHz), but could take as long as 16 seconds on a slow machine.

If any self test fails, the details of the failure are placed into the log and a message indicates a FIPS test failed (Figure 2). When you click on OK, the client exits.

Figure 2 Self test failure



Nortel VPN Client

FIPS 140-2 startup self test failed.
See the log for further details.

Self integrity check

Loaded application modules (such as Extranet.exe) can only run from the installation directory. This is to validate that the module on disk is the same as the one that is currently running.

For driver files (ipsecw2k.sys and eacfilt.sys), the on disk file in the window's system32/drivers directory is verified. Windows loads these files from this location so that the load path check is not required.

Known answer tests

The following KATs are be performed by the client application during startup:

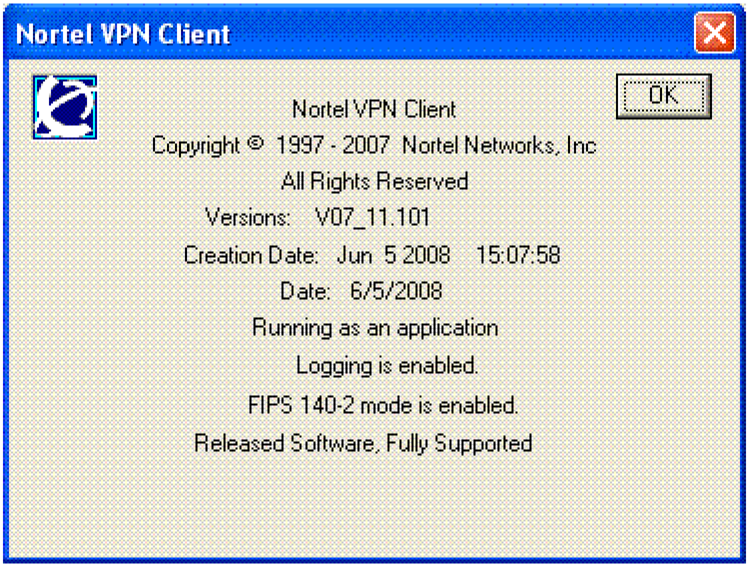
- 3DES
- AES(128 Bit)
- AES(256 Bit)
- SHA1
- HMAC-SHA1
- DH group 2 and 5
- PRNG

The driver runs its own KAT to verify the integrity of its encryption algorithms. If the test fails, no tunnels will be started.

FIPS mode status

The status of FIPS mode (enabled or disabled) is displayed in two places. In the main dialog, it is displayed in Help About (Figure 3).

Figure 3 Status in Help About



Nortel VPN Client

Copyright © 1997 - 2007 Nortel Networks, Inc

All Rights Reserved

Versions: V07_11.101

Creation Date: Jun 5 2008 15:07:58

Date: 6/5/2008

Running as an application

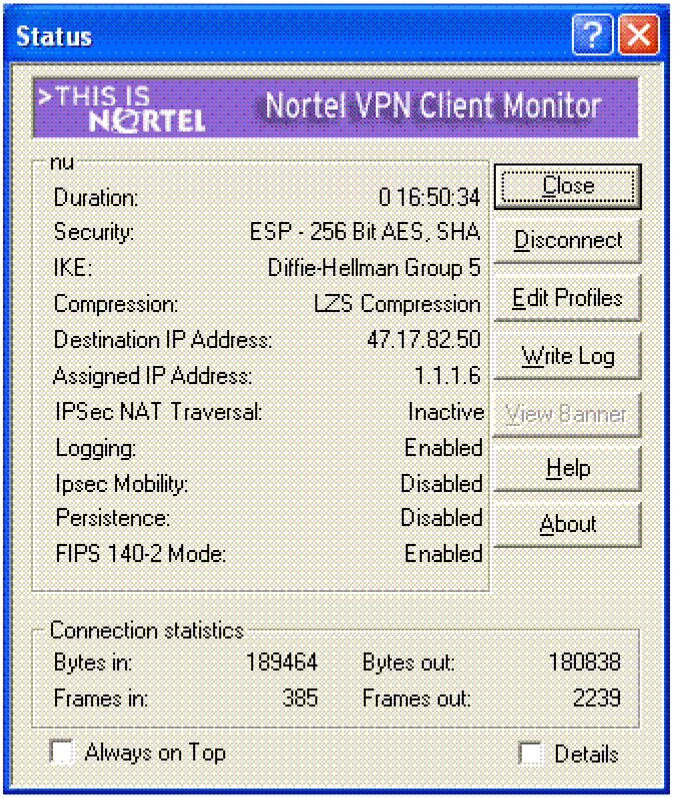
Logging is enabled.

FIPS 140-2 mode is enabled.

Released Software, Fully Supported

Once a tunnel has been established, it also displays in the status box (Figure 4).

Figure 4 Status box



nu

Duration: 0 16:50:34
Security: ESP - 256 Bit AES, SHA
IKE: Diffie-Hellman Group 5
Compression: LZS Compression
Destination IP Address: 47.17.82.50
Assigned IP Address: 1.1.1.6
IPSec NAT Traversal: Inactive
Logging: Enabled
Ipsec Mobility: Disabled
Persistence: Disabled
FIPS 140-2 Mode: Enabled

Connection statistics

Bytes in: 189464 Bytes out: 180838
Frames in: 385 Frames out: 2239

□ Always on Top □ Details

Continuous random number generator (RNG) test

FIPS requires that the RNG be continuously monitored to ensure it returns changing values. If RNG fails, the tunnel will be torn down.

Split tunneling mode

When FIPS mode is enabled, split-tunneling (both normal and inverse) is not allowed. If the server does send split tunneling routes during config mode, that information is ignored. The tunnel comes up but runs in mandatory tunneling mode. If this occurs, the following log entries are made:

```
Wed Dec 10 05:50:29 2008 | FIPS | W | Server is configured
for split tunneling but that is not allowed in FIPS mode.
Wed Dec 10 05:50:29 2008 | ConfMode | I | Mandatory
tunneling enforced.
```

The Avaya gateway continues as though the client is performing split-tunneling. It drops any packets that it determines should not have been sent through the tunnel. Even though the tunnel is established, the expected connectivity may not be there.

It is recommended that you configure groups for FIPS users or the server for mandatory tunneling.

Logging

Logging is mandatory in FIPS mode. The logging option under the Options, Log Sessions to File is checked to indicate that it is active and grayed out to prevent you from changing it.

The log contains the status of the FIPS mode and the results of the KAT and integrity checks.

```
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2 mode is
enabled.
Wed Dec 10 05:45:52 2008 | Isakmp | I | NVC Product Version
- V07_11.101
Wed Dec 10 05:45:52 2008 | Isakmp | I | Drivers' versions -
ipsecw2k.sys:7.11.0.101
; eacfilt.sys:7.11.0.101
Wed Dec 10 05:45:52 2008 | Isakmp | I | NVC executable
Version - 7.11.0.101
Wed Dec 10 05:45:52 2008 | Isakmp | I | Logging subsystem
initialized.
Wed Dec 10 05:45:52 2008 | Isakmp | I | Avaya VPN Client
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Hash
verification OK for file: C:\Program Files\Avaya\Avaya VPN
Client\extranet.exe
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Hash
verification OK for file: C:\Program Files\Avaya\Avaya VPN
Client\certal.dll
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Hash
verification OK for file:
C:\WINDOWS\system32\drivers\ipsecw2k.sys
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Hash
verification OK for file:
C:\WINDOWS\system32\drivers\eacfilt.sys
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Triple DES
KAT passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: AES (128
Bits) KAT passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: AES (256
Bits) KAT passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: SHA1 KAT
passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: HMAC-SHA1
KAT passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2:
Diffie-Hellman Group 2 KAT passed.
Wed Dec 10 05:45:53 2008 | FIPS | I | FIPS 140-2:
Diffie-Hellman Group 5 KAT passed.
Wed Dec 10 05:45:53 2008 | FIPS | I | FIPS 140-2: PRNG KAT
passed.
Wed Dec 10 05:45:53 2008 | FIPS | I | FIPS 140-2: Eacfilt
```

```
driver HMAC-SHA1 KAT and Integrity test passed.
Wed Dec 10 05:45:53 2008 | FIPS | I | FIPS 140-2: Ipsec
driver Triple DES, AES(128 Bits and 256 Bits), SHA1,
HMAC-SHA1 KAT passed.
Wed Dec 10 05:45:53 2008 | Isakmpd | I | Session End
Notification setup for XP :.
```

Supported DH groups and ciphers

The proposals made by the client in FIPS mode are, in order:

1. DH group 5: AES256-SHA1, AES128-SHA1.
2. DH group 2: 3DES-SHA1, AES128-SHA1.

The AesDisabled setup.ini is supported. If you set it along with FIPS mode, the client only proposes the group 2-3DES transform.

The following are not supported when running in FIPS mode:

- Diffie-Hellman group 8
- DES and DH group 1
- 40-bit DES
- MD5
- IPSEC AH

When you are running in FIPS mode, these will not be proposed by the client. The client rejects any proposal from the server that includes one of the unsupported groups or algorithms.

RSA and MSCAPI

The MSCAPI validates signatures when RSA certificates are used for authentication. To conform to FIPS, the client security policy states which versions of the Microsoft library have been FIPS-approved. The MSCAPI functions are provided by the rsaenh.dll library.

Disabling FIPS mode

Avaya VPN client version 7.11 operates in FIPS mode by default. To disable this mode, you have to run the custom install with the option NN_FIPSMODE=0.

For information on how to customize this installation, refer to *Avaya VPN Router Configuration — Client Version* 7.01 (NN46110-306) 311644-K Rev 02.

Index