Nortel Networks, Inc.
VPN Client Software

(Software Version: 7_11.101)

FIPS 140-2
Non-Proprietary Security Policy

Level 1 Validation

Document Version 0.5

Prepared for:

Nortel Networks, Inc.
600 Technology Park Drive
Billerica, MA 01821
Phone: (978)-670-8888
Fax: (978) 288-4004
http://www.nortel.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2007-05-15	Xiaoyu Ruan Darryl H. Johnson	Initial draft.
0.2	2008-02-21	Xiaoyu Ruan	Added algorithm certificate numbers.
0.3	2008-06-06	Xiaoyu Ruan	Version changed to 07_11.101.
0.4	2008-06-10	Xiaoyu Ruan	Addressed Lab comments.
0.5	2008-09-17	Darryl H. Johnson	Addressed Lab comments.

Table of Contents

Table of Figures

List of Tables

0 Introduction

0.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Virtual Private Network (VPN) Client Software from Nortel Networks, Inc. This Security Policy describes how the VPN Client Software meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/index.html.

The VPN Client Software is referred to in this document as the VPN Client, the Client Software, or the module.

0.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Nortel website (http://www.nortel.com/) contains information on the full line of products from Nortel.
- The CMVP website (http://csrc.nist.gov/groups/STM/index.html) contains contact information for answers to technical or sales-related questions for the module.

0.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Nortel. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Nortel and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Nortel.

1 VPN Client Software

1.1 Overview

The Nortel VPN Client provides the user-side functionality for secure remote access over Internet Protocol (IP) networks using Nortel IP access routers and VPN routers. The VPN Client ensures end-to-end network security by establishing a fully encrypted and authenticated VPN connection from a user's desktop across the Internet, terminating at a Nortel VPN router located at a trusted enterprise location.

The following table details the security level achieved by the VPN Client in each of the eleven sections of FIPS 140-2.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	Electromagnetic Interference/Electromagnetic Compatibility	3
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

The Nortel VPN Client is a software module composed of a set of binaries running on the Windows 2000 or Windows XP operating system on a general-purpose personal computer (PC). The module was tested for FIPS 140-2 requirements on Windows XP Professional with Service Pack (SP) 2. Testing was not performed on Windows 2000. In FIPS 140-2 terminology, the VPN Client is a multi-chip standalone module that meets the Level 1 FIPS 140-2 requirements.

Physically, the module is composed of the components of a general purpose PC, and the physical cryptographic boundary is the case of the PC. The PC or motherboard manufacturer could provide a block diagram for the exact hardware on which the module is installed, and the physical cryptographic boundary surrounds all of those components.

Logically, the VPN Client consists of the following four binaries running on Windows 2000 or Windows XP operating system (and the logical cryptographic boundary includes these four components, as depicted in Figure 1):

- VPN Client Application (extranet.exe) – Performs Internet Key Exchange (IKE) and provides a graphical user interface (GUI)
- IPSec Driver (ipsecw2k.sys) – Performs Internet Protocol Security (IPsec) functions
- Filter Driver (eacfilt.sys) – Filters traffic other than IKE and IPsec communications
- Library (CertAl.dll) – Interfaces with Microsoft Crypto Application Programming Interface (MSCAPI) for authentication using digital certificates

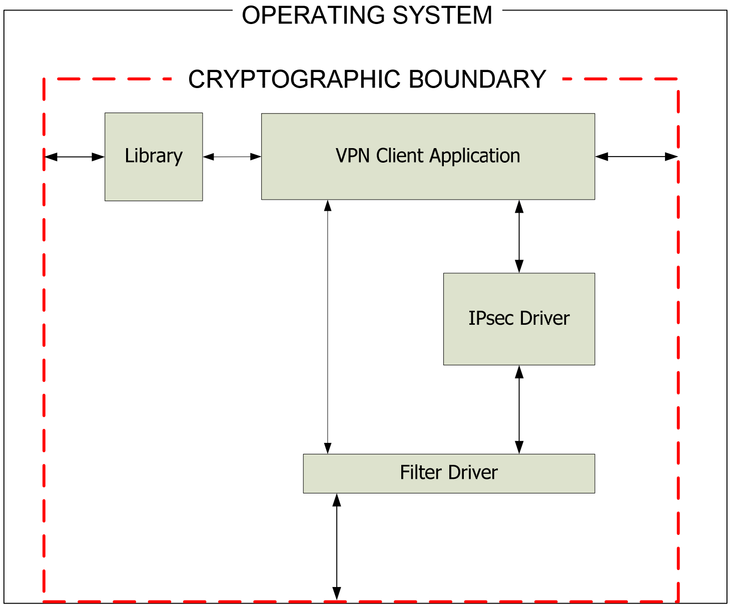

Figure 1 – Logical Block Diagram

1.2 Module Interfaces

The VPN Client Software's physical ports are those provided by the general purpose PC, including the Ethernet ports and mouse/keyboard ports. The Client's logical interfaces are composed of:

- GUI
- Command line interface (CLI)
- Application programming interface (API)
- Configuration and log files
- Packets traversing the networking stack

A mapping of the FIPS 140-2 logical interfaces to the VPN Client's logical interfaces and the physical interfaces of the PC can be found in the following table.

Table 2 – Mapping of Logical and Physical Interfaces

FIPS Logical Interface	VPN Client Logical Interface(s)	Physical Interface(s)
Data Input Interface	The data input is any data sent into the module through the networking stack to an application on the PC (such as email, browser, etc), and any data coming into the module through the networking stack from the network ports. Also, data input to the module via the MSCAPI for certificate processing and Rivest Shamir Adleman (RSA) algorithm operations.	Network ports

FIPS Logical Interface	VPN Client Logical Interface(s)	Physical Interface(s)
Data Output Interface	The data output is any data going out of the module through the networking stack from an application on the PC (such as email, browser, etc), and any data going out of the module through the networking stack out the network ports. Also, data output from the module to MSCAPI for certificate processing and RSA operations.	Network ports
Control Input Interface	Data read from configuration files, data input via the Nortel VPN Client GUI or CLI.	Keyboard port, hard disk, mouse ports
Status Output Interface	The Status Output is all error messages either logged by the module in a log file or the error messages in the GUI. The error messages from IKE negotiations are also status output. The logged error messages can be seen through the log files provided.	Light-emitting diodes (LEDs), hard disk, monitor ports

1.3 Roles and Services

The module supports role-based authentication. There are two roles in the module (as required by FIPS 140-2) that operators may assume: Crypto Officer and User.

1.3.1 Crypto Officer Role

The Crypto Officer role has the ability to install, uninstall, and configure the module's services using the GUI and CLIs provided by the module. Descriptions of the services (along with the inputs, outputs, critical security parameters (CSPs) and type of access for each) available to the Crypto Officer role are provided in the table below.

Table 3 – Mapping of Crypto Officer's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP	Type of Access
Install	Installing the VPN Client	Command options or Commands	Result of installation	Keyed-Hash Message Authentication Code (HMAC) - Secure Hash Algorithm (SHA1) for Integrity check	Read
Customize Client installation	Client software installation customization using setup.ini	Command options or Commands	Result of customization	None	None
Create a connection	To set up connection parameters	Command options	Status of command, response and results	Username and password	Read/Write
Profile data	To add/edit/delete a profile	Command options	Status of command, response and results	None	None

Service	Description	Input	Output	CSP	Type of Access
Authentication options	To authenticate to the Nortel VPN router	Command options or Commands	Command response	Username and password	Write
Name Server options	To specify a Domain Name Service (DNS) or Windows Internet Name Service (WINS) server, overriding the Nortel VPN router	Command option	Command response	None	None
KeepAlives	To enable or disable KeepAlive packets that maintain a connection during idle periods	Command options	Command response	None	None
Auto Connect	To Install/uninstall Auto Connect feature	Command options	Command response	None	None
Connect before logon	To enable or disable the Nortel VPN Client Graphical Identification and Authentication (GINA) dialog box on logon	Command options	Command response	None	None
Uninstall	To uninstall the software	Command options	Command response	All CSPs	Delete
Start/Stop	To start/stop the Nortel VPN Client services. The self tests are performed during the module start/restart.	Menu options or Commands	Status of command	HMAC-SHA1 for Integrity check	Read
Show status	Status messages for the module written to log file.	Commands	Status info in log file	None	None
Zeroization	Zeroizing CSPs	Uninstalling the module and reformatting the hard drive	Result of zeroizing	All CSPs	Delete

1.3.2 User Role

The User role has the ability to establish and utilize VPN sessions with a Nortel VPN router. Descriptions of the services available to the User role are provided in the table below.

Table 4 – Mapping of User’s Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP	Type of Access
VPN session	Use the VPN services	Encrypted/decrypted data	Encrypt/decrypted data	IPsec Session keys	Read/Write

Service	Description	Input	Output	CSP	Type of Access
Connect	To establish VPN session by authenticating to the Nortel VPN router	Authentication Information	Result of login attempt	Username and password	Read/Write
Edit profile	Edit the profile information on the Client	Command options	Updated profile information	Username and password	Read/Write
Change password	Change the current password used on the Nortel VPN router	Password	Updated password	Password	Write
Monitor Status	To monitor connection status	Command options	Status of command	None	None
Disconnect	To end the VPN session	Command options	Status of command	IPsec Session keys	Delete

1.4 Physical Security

The VPN Client Software is a multi-chip standalone cryptographic module. It is a software module and does not implement any physical security mechanisms.

Although the VPN Client consists entirely of software, the FIPS 140-2 tested platform is a standard PC which has been tested for, and meets, applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for home and business use as defined in Subpart B of FCC Part 15.

1.5 Operational Environment

The Nortel VPN Client was tested and validated on Windows XP, but it could run on either Windows XP or Windows 2000. For FIPS 140-2 compliance, these are considered to be single user operating systems. As such, all keys, intermediate values, and other CSPs remain only in the process space of the operator using the module. The operating system uses its native memory management mechanisms to ensure that outside processes cannot access the process space used by the module.

1.6 Cryptographic Key Management

The module utilizes the following FIPS-approved software algorithm implementations:

- Advanced Encryption Standard (AES) – Cipher-Block Chaining (CBC) mode (128, 256 bits) – FIPS 197 (certificate #721)
- Triple Data Encryption Standard (Triple-DES) – CBC mode (112, 168 bits) – FIPS 46-3 (certificate #644)
- Secure Hash Algorithm (SHA-1) – FIPS 180-2 (certificate #740)
- Keyed-Hash Message Authentication Code SHA-1 (HMAC-SHA1) – FIPS 198 (certificate #389)
- Pseudorandom Number Generator (PRNG) – General purpose implementation of FIPS 186-2 [(x-Original); (SHA-1)] (certificate #421)

In the FIPS mode of operation, the module utilizes the following non-Approved key agreement schemes. They are allowed by FIPS 140-2:

- Diffie-Hellman Group 2 (1024 bit), providing 80 bits of key strength
- Diffie-Hellman Group 5 (1536 bit), providing 96 bits of key strength

The module disables the following algorithm(s) when running in a FIPS mode of operation:

- Diffie-Hellman Group 8 (Elliptical Curve Discrete Logarithm (ECDL))
- Diffie-Hellman Group 1 (768 bit)
- Data Encryption Standard (DES)
- 40-bit DES
- Message-Digest Algorithm 5 (MD5)
- Keyed Hash Message Authentication Code MD5 (HMAC-MD5)

The following table lists all cryptographic keys, key components, and CSPs used by the module.

Table 5 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Integrity check HMAC-SHA1 key	HMAC (160 bits)	Externally generated predetermined value hard coded into the module	Never	Non-volatile memory (hard drive – plaintext) in module binaries in \isakmpd\fips.cpp	When the module is uninstalled or the hard drive is reformatted.	Software integrity check
FIPS 186-2 PRNG Seed key	Seed key (160 bits)	Generated internally by gathering system entropy	Never	Volatile memory only (plaintext)	When the module reboots	Used by FIPS 186-2 PRNG
Passwords	Alphanumeric string (minimum of 6 characters)	Externally created by an operator and entered into the module	Never	Volatile memory, or non-volatile memory (hard drive – plaintext)	By changing the password	Generate pre-shared keys for authentication during IKE
IPsec pre-shared keys	IPsec pre-shared key (160 bits)	Generated internally by HMAC of user ID and password	Never	Volatile memory only (plaintext)	When the module reboots	Mutual authentication between the module and the server
RSA public keys (Certificates)	RSA public key (1024–4096 bits)	Externally generated and input into and output from the module during IKE	During IPsec/IKE negotiation in plaintext	Volatile memory only (plaintext)	When the module reboots	Mutual authentication between the module and the server
IKE Diffie-Hellman key pair	Diffie-Hellman Group 2 (1024 bits) or Group 5 (1536 bits)	Generated internally during IKE	Never	Volatile memory only (plaintext)	When no longer used by the module or reboot	Used for session key agreement – public key sent to server
IKE Diffie-Hellman public key	Diffie-Hellman Group 2 (1024 bits) or Group 5 (1536 bits)	Exchanged during IKE	During IPsec/IKE negotiation in plaintext	Volatile memory only (plaintext)	When no longer used by the module or reboot	Used for session key agreement – received from server
IPsec session keys	AES (128, 256 bits) Triple-DES (112, 168 bits), HMAC-SHA-1 keys (160 bits)	Negotiated during IKE using Diffie-Hellman key agreement	Never	Volatile memory only (plaintext)	When no longer used by the module or reboot	Used to encrypt/decrypt/HMAC tunnel traffic

1.7 Self-Tests

The VPN Client performs the following self-tests at power-up:

- Software integrity check: Verifying the integrity of the software binaries of the module using an HMAC-SHA1 keyed hash.
- AES Known Answer Test (KAT): Verifying the correct operation of the AES algorithm implementation.
- Triple-DES KAT: Verifying the correct operation of the Triple-DES algorithm implementation.
- SHA-1 KAT: Verifying the correct operation of the SHA-1 algorithm implementation.
- HMAC-SHA1 KAT: Verifying the correct operation of the HMAC-SHA1 algorithm implementation.
- FIPS 186-2 PRNG KAT: Verifying the correct operation of the FIPS 186-2 PRNG implementation.

The VPN Client performs the following conditional self-tests:

- FIPS 186-2 Continuous Random Number Generator (RNG): Verifying that the Approved RNG does not repeatedly generate a constant value.
- Continuous RNG for entropy gathering: Verifying that the seed for the FIPS 182-2 PRNG does not repeatedly generate a constant value.
- Alternating bypass mode test: Verifying the integrity of the modules' bypass capability hardcoded in the filter driver.

The VPN Client will start its services only after all the self tests have passed. If the self tests have not passed, it enters an error state and logs the failure. All error conditions can be cleared by restarting the module.

1.8 Design Assurance

Nortel Networks uses the ClearCase Configuration Management System. The ClearCase software is used for software and document version control, code sharing, and build management. ClearCase also keeps track of what versions of files were used for each release and what combinations were used in builds.

Additionally, Microsoft Visual SourceSafe is used to provide configuration management for the VPN Client Software's FIPS documentation. This software provides access control, versioning, and logging.

1.9 Mitigation of Other Attacks

This section is not applicable. The VPN Client module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

2 Secure Operation

The VPN Client Software meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

2.1 Initial Setup

By default, the Nortel VPN Client is configured for a FIPS mode of operation.

2.2 Crypto Officer Guidance

The Crypto Officer is responsible for installation, customization configuration, management of the module, and removal of the module. More details on how to use the module can be found in the "Configuring the Nortel VPN Client" and "Using the Nortel VPN Client in FIPS Mode" documents.

2.2.1 Installation

The module uses RSA digital signature generation and verification as provided by the Microsoft Windows Operating System through the FIPS-approved MSCAPI libraries. However, the RSA functionality is not included inside the module; it is provided by one of the following FIPS-approved MSCAPI modules:

Table 6 – FIPS-Approved MSCAPI Modules Providing RSA Functionality

Certificate #	Windows Platform	rsaenh.dll Version
238	XP	5.1.2518.0 [XP] 5.1.2600.1029 [XP SP1] 5.1.2600.2161 {XP SP2]
103	2000 SPx	5.0.2150.1391 [SP1] 5.0.2195.2228 [SP2] 5.0.2195.3839 [SP3]
76	2000	5.0.2150.1

2.2.2 Management

By default, the Nortel VPN Client is configured for a FIPS mode of operation. The module can be put in a non-FIPS mode during custom installation or configuration. When switching between FIPS and non-FIPS modes, the operator must zeroize the group and user passwords by overwriting them with new values. Operators must not perform switching between FIPS and non-FIPS mode when using the module in a FIPS mode of operation. This should only be done during installation.

2.2.3 Zeroization

At the end of the life cycle of the module, the Crypto Officer must uninstall the module's software, overwrite all addressable locations with a single character, and reformat the hard drive which contained the software. This will zeroize all hard-coded keys and CSPs stored on the drive.

2.3 User Guidance

The User accesses the module's VPN functionality. The User must not modify the configuration of the module as established by the Crypto Officer, nor should a User reveal any of the CSPs (such as group and user passwords) used by the module to other parties.

3 Acronyms

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DES	Data Encryption Standard
DNS	Domain Name Service
ECDL	Elliptical Curve Discrete Logarithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
GINA	Graphical Identification and Authentication
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
KAT	Known Answer Test
LED	Light Emitting Diode
MD5	Message-Digest Algorithm 5
MSCAPI	Microsoft Crypto Application Programming Interface
NIST	National Institute of Standards and Technology
PC	Personal Computer
PRNG	Pseudorandom Number Generator
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SP	Service Pack
VPN	Virtual Private Network
WINS	Windows Internet Name Service